Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Enhancement of Cloud Data Protection using Attribute Based Encryption with Multiple Keys: A Survey

Md. Sameera[1,2] Dr. K. Usha Rani [3]
[1] Research Scholar, Dept. of Computer Science, Sri Padmavati Mahila Visvavidyalayam (SPMVV) (Women's University), Tirupati
[2] Lecturer, Dept. of Computer Science, D. K Govt. College for women (A), Nellore
Email : samee2016@gmail.com
[3] Professor, Dept. of Computer Science, Sri Padmavati Mahila Visvavidyalayam (SPMVV) (Women's University), Tirupati
Email : usharani.kuruba@gmail.com

Article Info
Page Number: 1952-1964
Publication Issue:
Vol. 72 No. 1 (2023)

Abstract:
Cloud Computing is an information technology innovation that enables clients to access system resources, computing power and storage on demand without the need for their direct supervision. It involves sending user data and application software to a remote data repository or cloud that users cannot directly control. As a result, users of cloud computing technology are mainly concerned with ensuring the protection and confidentiality of their information. Despite the growing popularity of cloud technology, there are still concerns about data security, privacy, reliability and interoperability that must be addressed. This article presents a survey conducted on the effectiveness of using Multiple Keys for a single file and the role of Attribute Based Encryption (ABE) with Multiple Keys, also known as Multi Authority Attribute Based Encryption (MA-ABE), in improving data security in the cloud. The survey examines how these techniques can be applied to increase the security of cloud based data, particularly in industries such as healthcare, finance, and government agencies that handle highly sensitive data and require strict access control.

Keywords: Cloud Computing, Access Control, Data Security, ABE, Multiple Keys, MA-ABE

Article History
Article Received: 15 April 2023
Revised: 24 May 2023
Accepted: 18 June 2023
Publication: 06 July 2023

I. INTRODUCTION

The term "cloud computing" describes the provision of computer services such as internet-based networking, software, data storage and servers. Companies and individuals can get these services on-demand from a cloud service provider rather than owning and maintaining physical data centres and servers. There are three primary classifications of cloud computing services, each offering unique advantages and customization options to meet the specific needs of different organizations. This enables users to access data and applications from anywhere with an internet connection and scale their usage up or down as needed.

1.1 Cloud Computing Services:

Cloud based services are categorized into three main groups depending on the level of

abstraction of services offered to customers. These categories include IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) as indicated in Fig.1 [1]. IaaS is a cloud computing service model where a third-party service provider hosts and manages infrastructure components such as servers, storage, networking, virtualization and other related resources on behalf of its clients or users. PaaS provides users with a complete software development environment over the internet including hardware and software tools. It allows developers to build, test and deploy software applications without the need to set up their own infrastructure. SaaS is a cloud computing service model where users can access and use software applications over the internet without having to install them on their local systems. This eliminates the need for clients to worry about software installation and allows them to use the desired software through a web browser or an application interface provided by the service provider. [2]. Users and organizations have a choice of Cloud Deployment Models to use for installing cloud services.

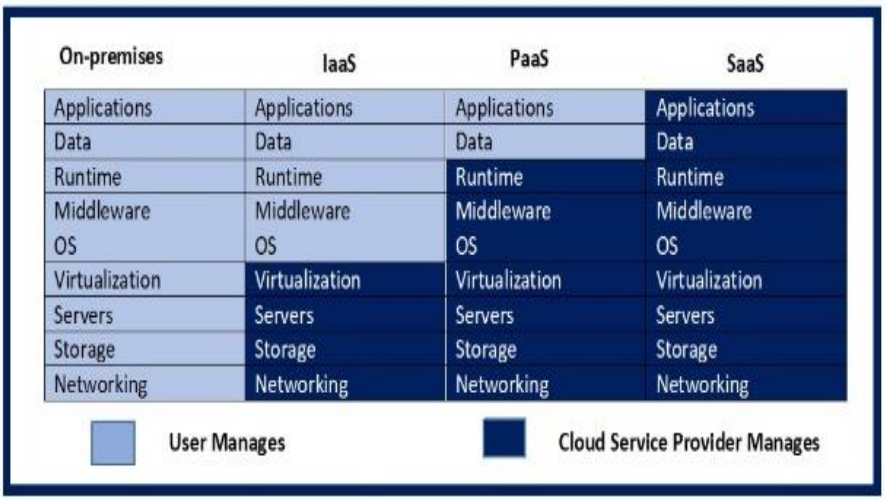

Fig. 1. Cloud Computing Services

1.2 Cloud Deployment Models:

Cloud Computing Deployment Models are primarily divided based on the location of the cloud infrastructure and the access level to the resources by users. There four main types of Cloud Delivery Models as depicted in Fig. 2. Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. The Public Cloud model allows all users to access services without any restrictions and they only pay for the services they use. The Private Cloud model offers services to a limited number of users, providing high levels of security through firewalls and internal hosting. Hybrid Cloud is an integration of both Public and Private clouds that can be managed independently, allowing for the sharing of data and applications between clouds. Finally, the Community Cloud model allows multiple organizations to share information by providing access to systems and services. Although cloud computing provides numerous benefits, it also presents several obstacles that must be resolved [2].

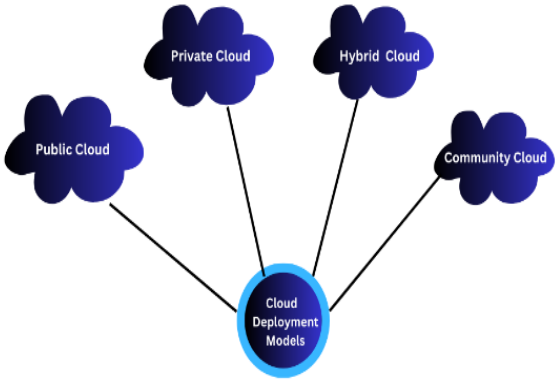

Fig. 2. Cloud Deployment Models

1.3 Top Cloud Challenges:

There are numerous difficulties with cloud computing. The Annual State of the Cloud Study on current cloud trends was recently completed by Flexera. They polled 997 technical personnel from a wide range of enterprises, asking them about their use of cloud infrastructure. Their study was informative, especially considering the challenges that cloud computing is presently encountering. According to this survey, the top cloud challenge is security, which ranks first with 85% of respondents which is clearly illustrated in Fig. 3. [3]. Consequently, this article presents a survey on data security.

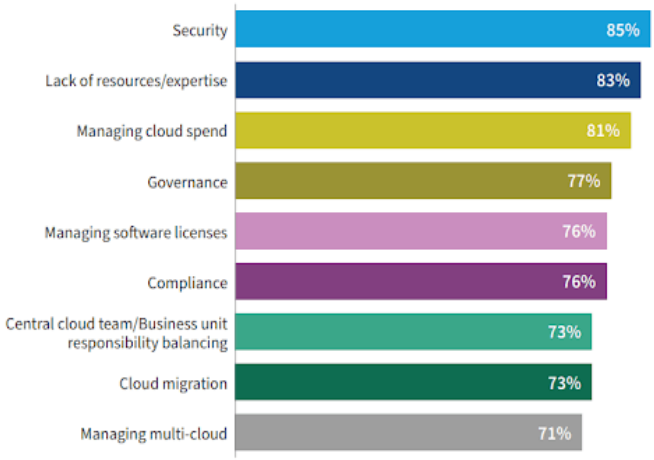

Fig. 3. Top Cloud Challenges [3]

1.4 Data Security:

Data security is a top priority for businesses using cloud computing services. Data protection solutions offered by cloud services include encryption, firewalls, and intrusion detection systems. But, enterprises must also take measures to guarantee the privacy, availability and integrity of their cloud-based data. Unauthorized access is one of the largest threats to data security in the cloud and can happen as a result of bad access controls, weak passwords or other flaws in the cloud environment. It is recommended for organizations to employ strong authentication techniques, such as multi-factor authentication and make sure that access

controls are configured effectively to reduce this risk. In order to prevent data breaches and other security issues, regular security audits and assessments can help to discover and address vulnerabilities in the cloud environment [4].

Another risk to data security in the cloud is data loss or corruption, which can occur due to hardware failures, software bugs or human error. To protect against this risk, organizations should implement data backup and recovery procedures, and regularly test these procedures to ensure they are effective [5]. One of the solution to enhance the data security is Cryptography which is foundation for information security.

1.5 Cryptography:

Cryptography is the art and science of converting plain text into a coded message to prevent unauthorized access to sensitive information. It is an essential tool in modern information security, used to protect confidential data during transmission and storage. Cryptography uses mathematical algorithms and protocols to guarantee the confidentiality, integrity and authenticity of data. In recent years, the development of advanced encryption techniques and the proliferation of digital communication have increased the importance of cryptography in securing sensitive information [6]. Asymmetric Encryption is a newer method compared to Symmetric Encryption. It was created to address the challenge of sharing keys in Symmetric Encryption models. Asymmetric Encryption uses a pair of public-private keys, so there is no need to share the key. However, Asymmetric Encryption is slower than Symmetric Encryption. [7]. Asymmetric key Encryption is not an optimal method for sharing a document with multiple users or groups. For instance, if a file needs to be shared with 100 users, it would require encrypting 100 copies of the file using each user's public key, which would be a computationally intensive task. Consequently, Attribute Based Encryption (ABE) is an alternative technique that is better suited for sharing documents with groups of users.

1.6 Attribute Based Encryption:

ABE is a powerful strategy to provide highly adaptable and precise access control for encrypted data. It does so by including access policies in the cipher text and private key, allowing one-to-many encryptions based on attributes. A given cipher text can only be decrypted by the designated private key if the involved attributes meet the policy requirements. By encrypting data with an access policy determined by the owner, ABE can be used to safely share data on the cloud. This guarantees that users who have been granted authorization with the matching attributes can only access the encrypted data on the cloud server. [8]. Another approach that can enhance data security in cloud computing involves generating multiple keys for a single file.

1.7 Multiple Keys:

Multiple key generation is another technique used to improve data security in the cloud by splitting a file into multiple fragments and generating a separate key for each fragment. So, if one key is compromised, only the corresponding data is affected, rather than the entire dataset. The keys are then distributed to authorized users to ensure that they can only access

their allocated fragment. In this way this technique also provides fine- grained access control [9].

The Subsequent sections of the paper are arranged in the following order: In Section 2, a taxonomy of ABE is presented. Section 3, focuses on the importance of Multiple Keys in ensuring data security. Section 4, explains ABE with Multiple Keys to enhance the data security and comparison of different MA-ABE techniques. Section 5, details the findings of the survey. Finally, Section 6 concludes the article.

II.TAXONOMY OF ABE

This section provides an explanation of various types of ABE along with their cryptographic functions.

The categorization of ABE consists of two main types: Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, the attributes are linked with the secret key, whereas in CP-ABE, the attributes are linked with the scrambled text. CP-ABE is further categorized into two types: Basic-CP-ABE and Enhanced-CP-ABE. The latter is divided into eight subtypes as shown in Fig. 4. which is briefly mentioned below [10].

1. Revocable CP-ABE: It allows revocation of access privileges for specific attributes or users. In this system it is possible through revocation authority to revoke access to certain attributes or users without affecting the security of the entire system.
2. Accountable CP-ABE: In Accountable CP-ABE, the encryption and decryption operations are performed by a trusted third party known as an accountability server.
3. Policy-Hiding CP-ABE: It provides an additional level of security by allowing the policy associated with a cipher text to be hidden from unauthorized users.
4. Policy Update CP-ABE**:** It is used to update the criteria for granting access involved in encoded data**.**
5. Multi-Authority CP-ABE: It allows the distribution of attribute authorities and delegation of attribute issuing rights among multiple authorities.
6. Hierarchical CP-ABE: Its capability is to facilitate more detailed and precise access control, along with the delegation of attribute issuing rights to various authorities in a hierarchical manner.
7. Offline/Online CP-ABE: This scheme allows for the decryption of messages in both offline and online modes.
8. Outsourced CP-ABE: It refers to a scenario where a user outsources the computation of a CP-ABE scheme to an external cloud service provider.

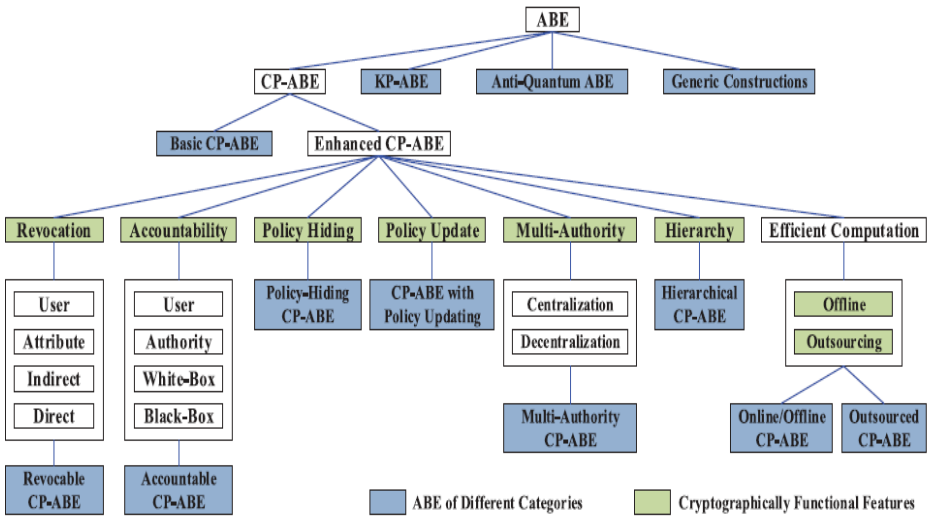

Fig. 4. Classification of ABE [10]

III. DATA SECURITY WITH MULTIPLE KEYS

A concise overview of different studies that employed the idea of generating multiple keys to improve the protection of data in cloud-based systems is presented here.

Gupta et al. [11] highlights the Multiple Encryption technique to enhance the security as well as integrity of confidential data. In this technique message digest which is generated after employing simple Hash algorithm on plaintext is encrypted multiple times with different encryption keys. The principal advantage of Multiple Encryption is that it enhances security by safeguarding the original data's confidentiality and privacy, even if some of the encryption keys or parts of the cipher text are compromised. This is the key benefit of Multiple Encryption.

Liu, Ximeng et al. [12] proposed a Privacy-Preserving Outsourced Calculation Toolkit that uses multiple keys to improve efficiency and security. The authors introduce a new key management mechanism that allows different keys to be used for different operations, such as addition, multiplication, and exponentiation. They also propose a secure and efficient protocol for outsourcing complex calculations to untrusted servers, while ensuring the privacy of the data and the correctness of the results. The proposed technique is evaluated through theoretical analysis and experimental results, which demonstrate its effectiveness in terms of security, efficiency, and scalability.

In the article Wang, Boyang et al. [13] authors present two effective methods for secure computation outsourcing on cloud data that is encoded using several keys. The authors proposed a scheme that allow polynomial functions to be computed over several end users' encoded data without the cloud servers learning the inputs, intermediate or final results. The schemes employ two non-colluding cloud servers and require limited interactions between them, making them practical for real-world applications such as machine learning and smart

metering. The authors demonstrate the efficiency of their schemes experimentally and argue that their approach can help users take advantage of the power of cloud computing while protecting their data privacy.

Peter et al. [14] proposed an efficient and secure technique for outsourcing secure multiparty computation to untrusted servers using Additively Homomorphic Encryption. The proposed method allows for the computation of any flexibly determined function on inputs that have been ciphered with multiple public keys, except for data upload and download. The output is produced through the use of a cryptographic protocol that is secure in the partly honest paradigm and is executed by two independent servers that are not colluding. The practicality of the method is demonstrated through two real-world applications: private smart metering and facial recognition that preserves user privacy

Gao, Chong-zhi et al. [15] suggested a privacy-preserving profile-matching protocol for mobile social networks with cloud assistance, where the profiles of users are encrypted under multiple keys to protect their privacy.

After analysing the above-mentioned articles, it became an evident that utilizing multiple keys for enhancing data security in cloud computing may lead to increased complexity in managing the keys and pose a risk of key loss or threats. Thus, in the subsequent section, we consider Attribute-Based Encryption (ABE) with Multiple Keys, particularly Multi-authority ABE (MA-ABE), which provides more flexibility in access control policies and helps reduce the burden of key management.

IV. DATA SECURITY USING ABE WITH MULTIPLE KEYS(MA-ABE)

ABE with Multiple keys is also known as Multi Authority ABE (MA-ABE). It allows multiple authorities to issue keys for the same cipher-text. In conventional ABE system, a single authority is responsible for issuing keys based on the attributes of the user. However, in MA-ABE system, multiple authorities can collaborate to issue keys based on their respective attributes. It allows for more flexible access control policies, as authorities can issue keys based on different criteria and can enforce different policies. It also enhances security, as a compromised authority cannot decrypt the cipher-text without collaboration of other authorities. Table-1 presents several instances of attributes along with the respective attribute authorities accountable for their management.

Table 1: An example of attributes and the authorities which handles them in reality

Attribute	**Attribute Authority**
Education Degree	Accreditation board or educational institution
Medical Records	Healthcare Provider or Hospital
Financial Credit Score	Credit Bureaus or Financial Institutions
Driver’s license	Driver licensing authority
Vehicle Registration	Department of Motor Vehicles

MA-ABE has been utilized in several articles to increase the security of data in cloud environments, and a few of these articles are listed below.

The article Chase et al. [16] highlights the traditional ABE which relies on a single authority to manage access control polices and issue decryption keys and also proposed a new encryption scheme with multiple authorities and proves its security properties including collusion resistance and user revocation. Overall, the article demonstrates the potential benefits of MA-ABE in terms of flexibility, scalability and security.

Chase et al. [17] presented a resolution to the issue of MA-ABE using a trusted Central Authority (CA) and Global Identifiers (GID). However, this approach had a drawback as it gave the complete authority to decrypt all cipher-text, which goes against the initial objective of dispersing power among multiple authorities. To address this problem, the authors introduced a new solution that eliminates the requirement for a dependable central authority and safeguards the privacy of users by stopping authorities from aggregating data about particular individuals. This makes ABE more practical for real-world applications.

Lin, Huang et al. [18] explains about Multi Authority Fuzzy Identity Based Encryption (MA-FIBE) scheme without the need for a sole decision-making entity. The proposed method uses a distributed key generation algorithm to distribute the authority among multiple authorities, each with its own set of attributes. This allows for a more flexible and scalable ABE system that can handle a large number of attributes and authorities. Additionally, the method includes a threshold scheme to ensure that access to the encrypted data requires a minimum number of authorities to cooperate. The authors conduct a security analysis of the proposed method and compare it with other existing approaches.

The article by Li, Jin et al. [19] presents a method known as MA-ABE with Accountability, which enables for the identification of a user who has leaked decryption keys to unauthorized individuals. The process of tracing is effective and the computational burden is directly relative to the user's identity.

Bozovic et al. [20] describe a Multiple-Authority ABE scheme that eliminates the need for a central authority that can be trusted. This scheme is an extension of the Solo Authority ABE scheme introduced earlier by Sahai and Waters, and it is based on the Bilinear Diffie-Hellman assumption. The proposed method ensures that only the group of receivers specified by the entity or person performing the encryption can decode the corresponding encrypted message. The CA in this scheme is assumed to be both sincere and inquisitive, meaning that it follows the protocol faithfully but may be interested in decrypting arbitrary cipher-texts.

In the research article Parvatikar et al. [21] authors proposed a secure method for sharing Personal Health Records (PHRs) using MA-ABE to the users based on attributes in cloud computing. The importance of protecting the privacy and confidentiality of PHRs and challenges of sharing them among health care providers is also discussed in this article.

Lakshmi et al. [22] tackle an important problem in CP-ABE, which is revocation. Their proposed solution allows for the revocation of user attributes by the Multi Authority with minimal effort. This is accomplished by integrating proxy re-encryption with CP-ABE in a unique manner, which allows the person in charge to assign the difficult tasks to proxies.

Rouselakis et al. [23] proposed a system which is an efficient large-scale MA-ABE scheme that allows the use of any character string as an attribute and doesn't necessitate a central body for key distribution. It achieves great flexibility by enabling multiple sources of authority to manage the circulation of keys for a vast number of attributes in an exponential manner and its cipher-text policies are sufficiently expressive to overcome previous restrictions. The construction uses bilinear groups with the same prime order to increase efficiency and is proven to be secure in the random oracle model without responding to the other party's actions, based on q-type assumption without any communication. It expands on previous approaches and introduces two new techniques that can be utilized in other ABE constructions. The system has been implemented and benchmarked in the Charm programming framework.

Chow et al. [24] presents a plan for building MA-ABE systems with Attribute Revocation and Outsourced Decryption. This plan can be applied to any single-authority ABE scheme that meets specific criteria outlined in the paper. The proposed framework is designed with the goal of improving the security and scalability of ABE systems by allowing multiple authorities to manage different attributes and by enabling the revocation of attributes. Additionally, the framework facilitates outsourced decryption, which enables a user to outsource decryption operations to a third party.

Belguith, Sana et al. [25] developed a scheme called Policy-Hidden Outsourced ABE (PHOABE) that allows a Semi-Trusted Cloud Server to perform complex computations, while keeping users' privacy protected with a hidden access policy. PHOABE is a secure and verifiable scheme that preserves policy privacy under the random oracle model. The authors demonstrated that PHOABE is practical for use in IoT constrained environments.

Oberko et al. [26] provides a comprehensive survey of traditional ABE and MA-ABE schemes over the past decade, including design principles, techniques and algorithms. It also discusses the progress and extension of MA-ABE and compares previous research in the fields of security, efficiency and capabilities. The study identifies open problems and provides insights into the state-of-the-art of MA-ABE.

In summary, Table 2 presents a comparison of different MA-ABE schemes, highlighting their various features and functionalities. The purpose of the table is to assess and analyse the characteristics and capabilities of these schemes.

Table 2: Comparison of Existing MA-ABE Schemes

Reference	Scheme	Access Control Model (CP/KP/DP ABE)	Group Order	Access Structure	Security Model	RO/ Standard Model	Key Issuing Protocol	LU Support	Assumption
[16]	MA-ABE	KP-ABE	Prime	Threshold	Non-Adaptive	Standard	GID	Yes	BDH
[17]	MA-ABE (without CA and GID)	KP-ABE	Prime	Tree	Non-Adaptive	RO	Anonymous	Yes	DBDH
[18]	MA-FIBE	DP-ABE	Prime	Threshold	CPA secure under selective set model	Standard	-	Yes	DBDH
[19]	MA-ABE with Accountability	CP-ABE	Prime	AND gates with Wild card	Non-Adaptive (Selective Security Model)	Standard	Anonymous	No	DBDH DLIN q-DDHI
[20]	MA-ABE (with Honest & Curious CA)	CP-ABE	Prime	Threshold	Selective ID Model	RO	-	No	DBDH
[22]	MA-ABE with Attribute Revocation	CP-ABE	-	AND gates	CCA Secure	RO	GID	No	-
[23]	Large Scale MA-ABE	CP-ABE	Prime	LSSS	Non-Adaptive (Static Model)	RO	GID	Yes	q-type
[24]	MA-ABE with Outsourcing and Revocation	DP-ABE	Composite	LSSS	Adaptive (Stronger Security Model)	RO	GID	Yes	-
[25]	PHOABE	CP-ABE	Prime	LSSS	Selectively Secure Model	RO	GID	No	CDH DBDH

Key: LSSS: Linear Secret Sharing Scheme, GID: Global Identifiers, RO: Random Oracle, CPA: Chosen Plaintext Attack, CCA: Chosen Cipher text Attack, BDH: Bilinear Diffie-Hellman, DBDH: Decisional Bilinear Diffie-Hellman, DLIN: Decisional Linear, q-DDHI: q-Decisional Diffie-Hellman Inversion CDH: Computational Diffie Hellman

V. FINDINGS OF THE SURVEY

In this section, Table 3 presents the main outcomes and observations derived from the survey conducted on MA-ABE techniques for improving cloud data security.

Table 3: Survey Findings

Reference	Scheme	Brief Description	Limitations/Future Scope
[16]	MA-ABE	• This scheme explains how polynomial number of multiple authorities used to monitor attributes and distribute secret keys • It also presents multi authority version with large universe fine grained access control	The limitation of this scheme is that it requires each authority's attribute set to be disjoint. Therefore, it is necessary to create separate copy of each attribute for each clause in which it could possibly appear.
[17]	MA-ABE (without CA and GID)	• It addresses a drawback of using trusted central authority. • It presents a solution by eliminating the central authority which has complete control to decrypt the cipher text. • It safeguards the privacy of users by stopping authorities from aggregating data about particular individuals. • Therefore, ABE becomes more practical for real-world applications.	-

[18]	MA-FIBE	• Provides a threshold MA-FIBE scheme without a central authority. • A distributed key generation algorithm is employed to distribute authority among multiple entities, with each entity possessing its unique set of attributes.	Incorporating new authorities without causing any trouble to users remains an unresolved issue.
[19]	MA-ABE with Accountability	It focuses on tracing the identity of misbehaving user.	Tracing the identity of the misbehaving user is computationally over head as the length of the identity increases.
[20]	MA-ABE(with Honest & Curious CA)	• It ensures that only the group of receivers specified by the entity or person performing the encryption can decode the corresponding encrypted message. • The CA is viewed as honest- but -curious meaning that it follows the protocol faithfully but may be interested in decrypting arbitrary cipher-texts.	-
[22]	MA-ABE with Attribute Revocation	• It enables efficient attribute revocation method with both forward and backward security • The computation of decryption is outsourced to the online proxy-server.	Future work will focus on resolving the weaknesses associated with forward and backward security.
[23]	Large Scale MA-ABE	• It is large universe MA-CPABE scheme • Any string can be used as attribute of the ABE system • No Central Authority • Several Attribute Authorities are responsible for authorized key distribution. • It overcomes the restriction to use each attribute is used only once • Provided implementation on charm programming frame work	-

[24]	MA-ABE with Outsourcing and Revocation	• An abstraction of ABE which can be extended to support set of nice features namely
		  • Multi Authority Extension
		  • Attribute Level Revocation
		  • Outsourced Decryption
		• Also explains the set of properties for the correctness and security of the proposed approach
			• Reducing the key-update materials for attribute level revocation is appears to be challenging in multi authority setting.
			• Another challenge is to explore the feasibility of outsourced decryption for anonymous ABE, where the policy linked to the cipher text remains undisclosed to any intermediary.

[25]	PHOABE	It allows a Semi-Trusted Cloud Server to perform complex computations, while keeping users' privacy protected with a hidden access policy	Enhancement of PHOABE with direct revocation approach enables to revoke the compromised user without affecting other users .
[26]	MA-ABE	• Survey on traditional ABE as well as MA-ABE is done in this article • Design Principles of MA-ABE is mentioned • Mentioned comparison between existing works on areas as security, performance etc.,	• More constructions of ABE and MA-ABE with lattices or any other harder mathematical problem is required to achieve high level of security in this quantum computing era. • Designing of MA-ABE based on multi-linear groups has the possibility of solving the quantum computing problem. • Developing practical multi-authority attribute-based encryption (ABE) schemes within decentralized systems would be a highly favourable concept due to its ease of implementation in real-world scenarios.

VI. CONCLUSION

Ensuring the confidentiality and integrity of sensitive data is a significant challenge in cloud computing. This study addresses data security in the cloud and investigates the utilization of Multiple Keys generation for a single file and Multi-Authority Attribute-Based Encryption (MA-ABE) as potential solutions. The survey conducted reveals that while generating multiple keys can enhance data security, it imposes a heavy burden on key management. Consequently, MA-ABE emerges as a promising approach as it allows data encryption based on attributes, leading to improved data security, flexibility, and scalability while reducing the complexity of key management. Moreover, MA-ABE proves to be cost-effective by utilizing cloud-based key management systems. The primary objective of this survey is to extensively analyse and evaluate various multi-authority schemes documented in existing literature, aiming to provide a comprehensive understanding of their capabilities and functionalities. However, additional research is necessary to enhance the efficiency and scalability of MA-ABE schemes and address emerging security threats in cloud computing.

REFRENCES

[1]. Gupta, I., Gurnani, D., Gupta, N., Singla, C., Thakral, P., & Singh, A. K. (2022). Compendium of data security in cloud storage by applying hybridization of encryption algorithm.

[2]. M.d.Sameera, Dr. K. Usha Rani, "A Review on Data Security in Cloud Environment with Artificial Intelligence", DE, pp. 15819 - 15830, Jan. 2022.

[3]. Top Challenges of cloud computing: https://www.datapine.com/blog/cloud-computing-risks-and-challenges/

[4]. Krutz, R. L., Krutz, R. L., & Russell Dean Vines, R. D. V. (2010). *Cloud security a comprehensive guide to secure cloud computing*. Wiley.

[5]. Mather, Tim, Subra Kumaraswamy, and Shahed Latif. *Cloud security and privacy: an enterprise perspective on risks and compliance*. " O'Reilly Media, Inc.", 2009.

[6]. Menezes, A. J., & van Oorsschoot, P. C. (1996). Vansto e, SA. *Handbook of applied cryptography*.

[7]. Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.

[8]. Xiong, H., Zhang, H., & Sun, J. (2018). Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. *IEEE Systems Journal*, *13*(3), 2739-2750.

[9]. Wang, B., Li, M., Chow, S. S., & Li, H. (2013, October). Computing encrypted cloud data efficiently under multiple keys. In *2013 IEEE Conference on Communications and Network Security (CNS)* (pp. 504-513). IEEE.

[10]. Zhang, Y., Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based encryption for cloud computing access control: A survey. *ACM Computing Surveys (CSUR)*, *53*(4), 1-41.

[11]. Gupta, H., & Sharma, V. K. (2011). Role of multiple encryption in secure electronic transaction. *International Journal of Network Security & Its Applications*, *3*(6), 89.

[12]. Liu, X., Deng, R. H., Choo, K. K. R., & Weng, J. (2016). An efficient privacy-preserving outsourced calculation toolkit with multiple keys. *IEEE Transactions on Information Forensics and Security*, *11*(11), 2401-2414.

[13]. Wang, B., Li, M., Chow, S. S., & Li, H. (2013, October). Computing encrypted cloud data efficiently under multiple keys. In *2013 IEEE Conference on Communications and Network Security (CNS)* (pp. 504-513). IEEE.

[14].Peter, A., Tews, E., & Katzenbeisser, S. (2013). Efficiently outsourcing multiparty computation under multiple keys. *IEEE transactions on information forensics and security*, *8*(12), 2046-2058.
[15].Gao, C. Z., Cheng, Q., Li, X., & Xia, S. B. (2019). Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network. *Cluster Computing*, *22*, 1655-1663.
[16].Chase, M. (2007). Multi-authority attribute based encryption. In *Theory of Cryptography: 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007. Proceedings 4* (pp. 515-534). Springer Berlin Heidelberg.
[17].Chase, M., & Chow, S. S. (2009, November). Improving privacy and security in multi-authority attribute-based encryption. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 121-130).
[18].Lin, H., Cao, Z., Liang, X., & Shao, J. (2010). Secure threshold multi authority attribute based encryption without a central authority. *Information Sciences*, *180*(13), 2618-2632.
[19].Li, J., Huang, Q., Chen, X., Chow, S. S., Wong, D. S., & Xie, D. (2011, March). Multi-authority ciphertext-policy attribute-based encryption with accountability. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 386-390).
[20].Božović, V., Socek, D., Steinwandt, R., & Villányi, V. I. (2012). Multi-authority attribute-based encryption with honest-but-curious central authority. *International Journal of Computer Mathematics*, *89*(3), 268-283.
[21].Parvatikar, S., Prakash, P., Prakash, R., Dhawale, P., & Jadhav, S. B. (2013). Secure sharing of personal health records using multi authority attribute based encryption in Cloud Computing. *International Journal of Recent Advances in Engineering\& Technology (IJRAET)*, *5*, 50-52.
[22].Lekshmi, S. V., & Revathi, M. P. (2014, February). Implementing secure data access control for multi-authority cloud storage system using Ciphertext Policy-Attribute based encryption. In *International conference on information communication and embedded systems (ICICES2014)* (pp. 1-6). IEEE.
[23].Rouselakis, Y., & Waters, B. (2015, July). Efficient statically-secure large-universe multi-authority attribute-based encryption. In *Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers* (pp. 315-332). Berlin, Heidelberg: Springer Berlin Heidelberg.
[24].Chow, S. S. (2016, June). A framework of multi-authority attribute-based encryption with outsourcing and revocation. In *Proceedings of the 21st ACM on symposium on access control models and technologies* (pp. 215-226).
[25].Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., & Attia, R. (2018). Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. *Computer Networks*, *133*, 141-156.
[26]. Oberko, P. S. K., Obeng, V. H. K. S., & Xiong, H. (2022). A survey on multi-authority and decentralized attribute-based encryption. *Journal of Ambient Intelligence and Humanized Computing*, 1-19.