International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 21s, 2025
https://www.theaspd.com/ijes.php

Issues and Challenges in Ciphertext-Policy Attribute-Based Encryption for Secure Cloud Storage

Siti Dhalila Mohd Satar[1,3], Masnida Hussin[2], Mohamad Afendee Mohamed[1], Nazirah Abd Hamid[1], Ahmad Faisal Amri Abidin[1], Nor Aida Mahiddin[1,3]
[1]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terengganu, Malaysia
[2]Faculty of Information Technology and Computer Science, Universiti Putra Malaysia, Selangor, Malaysia
[3]East Coast Environmental Research Institute, Universiti Sultan Zainal Abidin, Terengganu, Malaysia, sitidhalila@unisza.edu.my

Abstract

The rapid growth of cloud computing has revolutionized data storage, offering significant benefits in terms of scalability and accessibility. However, these advantages come with critical security challenges, particularly in ensuring data confidentiality and access control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has emerged as a promising solution to these challenges. This paper provides a comprehensive review of the key issues associated with CP-ABE in cloud storage, focusing on ciphertext size, multi-authority architecture, user revocation, and access policy hiding. Through an extensive literature review spanning studies from 2015 to 2023, we identify current solutions and highlight their limitations. Our analysis reveals that while significant progress has been made in reducing ciphertext size and improving multi-authority systems, challenges remain in efficient user revocation and robust access policy hiding. Key results indicate that hybrid encryption techniques and dynamic policy updates are effective in addressing some of these issues. The implications of our findings suggest that future research should focus on enhancing these techniques and developing more integrated approaches to overcome the persistent challenges in CP-ABE, thereby improving the security and efficiency of cloud storage systems.

Keywords: *Access control, Ciphertext Policy Attribute based Encryption (CP-ABE), CP-ABE issues, Cloud Security, Cloud Storage.*

1. INTRODUCTION

The Cloud computing paradigm has grown in popularity in both industry and academia since its inception. Cloud computing has many impressive characteristics, such as being economical, scalable, expedient, ubiquitous, on-demand access, and location-independent for shared resources [1–3]. As a result of these characteristics, the company has decided to move its business functions to the Cloud. Cloud computing allows computer resources to be delivered as IT services in a pay-as-you-go model that seeks to provide high availability, reliability, vast scalability, and data sharing at a very low cost.

Cloud storage, a prominent service provided by cloud computing, enables users to outsource their data for storage or sharing. As indicated in works [4-5], the cloud services provider is responsible for managing the physical data and the equipment associated with cloud storage. Meanwhile, users retain a certain level of control over the virtual machines. However, this arrangement can pose a risk to data owners' privacy in terms of data storage, owing to the limited control they have over data security.

In the Cloud storage, the privacy of data is very challenging to preserve and ensuring data availability while maintaining its security much more challenging to provide. The Cloud Service Provider (CSP) is often considered an untrusted entity that could potentially have malicious intentions towards data stored in the Cloud. A CSP might engage in malicious activities, either deliberately by charging for all data and removing unaccessed data following a usage analysis, or by maintaining fewer replicas than agreed upon. Additionally, there are instances where the CSP might unintentionally overlook issues such as the creation of bad sectors on the disk or a hard disk crash, as noted in references [6-8]. All these activities may damage the security of the data. To counter these security challenges, various solutions like cloud data encryption, secure access management, and privacy-aware authentication have been developed [9-12]. These measures are crucial in ensuring ongoing research focuses on enhancing security in cloud storage, striking a balance between robust protection and efficient resource utilization.

Therefore, this paper seeks to conduct a comprehensive examination of the critical issues related CP-ABE. The objective of conducting an in-depth analysis on existing schemes, focusing on attribute revocation, access policy obfuscation, ciphertext size, and multi-authority concerns, is to identify and analyse the current issues and areas of focus among researchers regarding the CP-ABE scheme and to understand the solutions and developments proposed by existing works. The insights gained from this analysis are tailored to offer practitioners guidance in the wise selection and skilful implementation of security mechanisms, thereby ensuring optimal data security reinforcement in their organizational framework. Such a strategic approach is not only beneficial but essential for upholding the integrity and confidentiality of an organization's data in the complex cloud landscape. In conclusion, this paper advances the discourse on CP-ABE, providing nuanced understanding and actionable insights for both practitioners and researchers in the field of secure cloud computing.

The rest of the paper is structured as follows. Section 2 discussed on CP-ABE while Section 3 elaborated in the methodology. Section 4 presents detail CP-ABE issues. Section 4 concludes the study and includes recommendations for further work.

2. Ciphertext Policy Attribute based Encryption in Cloud Storage

There are several forms of Attribute-Based Encryption (ABE), with Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) being the most notable. KP-ABE, introduced in [13], is tailored for one-to-many communications. In this system, the encryptor labels each ciphertext with a set of attributes, and each private key is linked to an access structure that determines which ciphertexts it can decrypt. A user can decrypt and access the data if the attributes of the encrypted data align with the access control policy of their private key. On the other hand, CP-ABE, proposed in [14], presents an alternate approach. CP-ABE embeds the access control policy within the encrypted data itself, whereas the user's private key is defined by certain attributes. Here, users can decrypt and access the data if their attributes match the access policy of the encrypted data.

This paper directs its focus towards CP-ABE over KP-ABE due to CP-ABE's considerable attention in practical applications, especially within cloud storage and data sharing environments, owing to its inherent adaptability. However, CP-ABE encounters challenges in meeting access control requirements that necessitate flexibility, efficiency, and the capability to accommodate diverse users, extensive datasets, and intricate security needs [15-16]. Table 1 presents a summarization of CP-ABE in comparison to KP-ABE.

Table 1. Summarization of CP-ABE with KP-ABE

Parameters	**CP-ABE**	**KP-ABE**
Access Control	Based on attributes of ciphertext	Based on attributes of decryption key
Encryption Policy	Associated with ciphertext	Associated with decryption key
Attribute Usage	Attributes associated with both data and users	Attributes associated with data

Decryption Process	Requires attributes matching the policy associated with ciphertext	Requires attributes matching the policy associated with decryption key
Scalability	Suitable for scenarios with many data users	Suitable for scenarios with many data policies
Computational Overhead	May involve higher computational overhead due to complex access control policies	Involve lower computational overhead as access policies are associated with decryption key

Ciphertext Policy Attribute-Based Encryption (CP-ABE) as shown in Figure 1 is an encryption scheme enhancing data confidentiality and controlling access to the cloud storage. It enables fine-grained access by linking attributes to users and data, forming flexible policies for data access based on user attributes [17]. The data is encrypted under an access policy, allowing decryption only by users with matching attributes. This approach ensures that confidential data can be securely stored on untrusted servers [18-19].

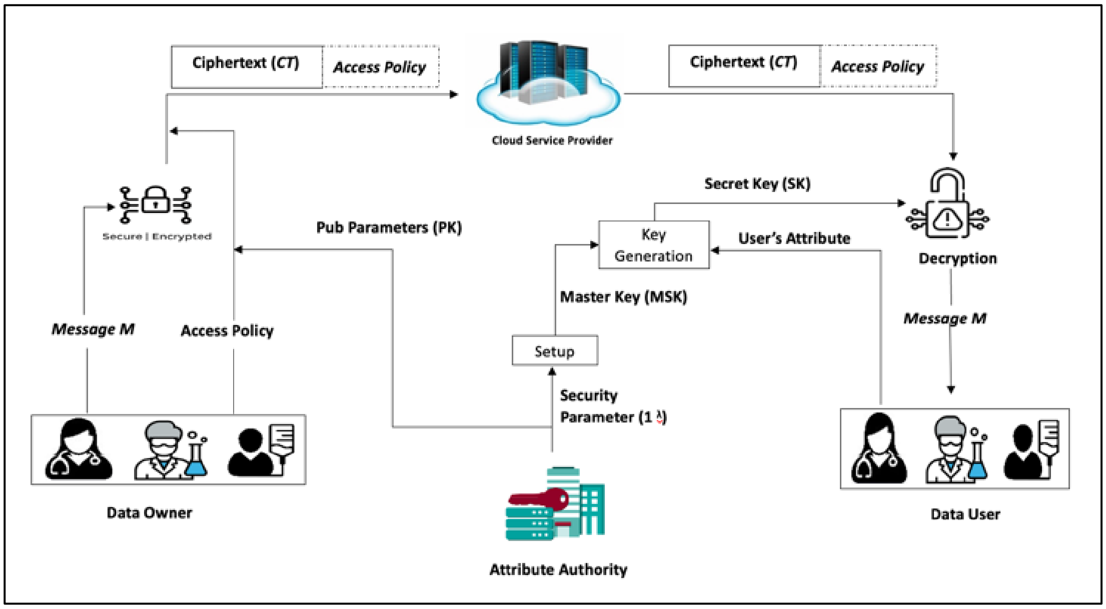

Fig. 1 CP-ABE Architecture

CP-ABE stands out from traditional encryption methods, especially in scenarios needing detailed access control. It integrates seamlessly with cloud services, offering precise and secure data protection policies. However, the complexity of CP-ABE's implementation and maintenance poses significant challenges [20]. Its attribute-based access control system requires meticulous design and management, which can increase vulnerability risks.

Another major concern is CP-ABE's computational overhead. The encryption and decryption processes are resource-intensive, potentially affecting system performance, particularly in resource-limited environments or with large datasets [21]. Additionally, CP-ABE grapples with issues like privacy leakage in access policies, large ciphertext size, and policy revocation challenges. Despite these challenges, CP-ABE remains a critical tool in cloud security, and ongoing research is directed at addressing its limitations to enhance its efficiency and real-world applicability. Researchers are actively exploring solutions to mitigate its complexity, computational overhead, and other operational challenges.

3. METHODOLOGY

In this study, the methodology outlined in Figure 2 is employed to critically analyze the CP-ABE scheme. The approach begins with a comprehensive search in bibliographic databases like ACM Digital Library, IEEE Digital Library, and Google Scholar using "cp-abe" as the primary keyword. Following this, a thorough examination of references within each publication was conducted to compile a comprehensive list of works related to the CP-ABE scheme. Any publications that did not specifically address issues in CP-ABE were subsequently excluded from the catalogue. Subsequently, publications are categorized based on specific CP-ABE issues, and each issue is analysed in depth, allowing for a thorough and structured exploration of the CP-ABE scheme's complexities.

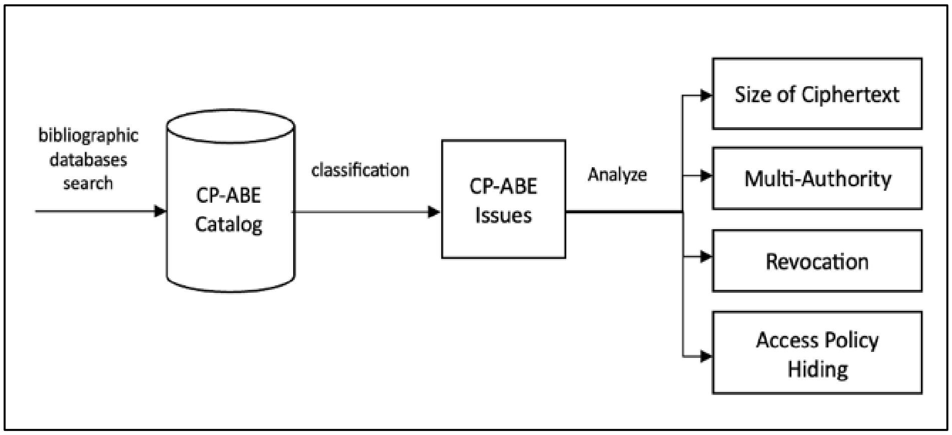

Fig. 2 Research Methodology

4. Implementation Challenge of CP-ABE in Cloud Storage

There are several issues in CP-ABE. These issues include revocation, multi-authority, ciphertext size, key size, traceability, and access policy hiding. To address these issues, various improvement solutions in CP-ABE have been proposed. Each of these proposed solutions has its own strengths and weaknesses. The strengths can be leveraged, while the weaknesses can be improved upon. The following subsection provides a more detailed explanation of the issues in CP-ABE.

4.1. Size of Ciphertext

In CP-ABE, the issue of large ciphertext sizes is of significant concern. In many existing CP-ABE schemes, the size of the ciphertexts grows with the number of attributes included in the access policy which stems from the use of a Boolean access policy. This results in larger ciphertexts, which in turn cause increased computational burdens and heightened security risks [22-23].

The problem of large ciphertexts is not merely a matter of inconvenience or storage inefficiency. It has practical implications that need to be addressed. Firstly, large ciphertext sizes can impose a considerable computational burden on the system. The encryption and decryption processes become more time-consuming, requiring additional computational resources. This can hinder the efficiency and scalability of the CP-ABE scheme, especially when dealing with a large number of attributes and users.

Moreover, the increased ciphertext size poses security risks. The transmission and storage of large ciphertexts require more bandwidth and storage space, potentially impacting the overall performance and cost-effectiveness of the system. Additionally, large ciphertexts may attract more attention and scrutiny from adversaries, increasing the likelihood of attacks or attempts to exploit vulnerabilities.

To mitigate these challenges, researchers have proposed various techniques to reduce ciphertext size or maintain a constant size. [24] introduced a lightweight and verifiable access control scheme applicable to achieve constant size of ciphertexts. This scheme aims to reduce the burden on end users by providing constant size ciphertext, thus addressing the challenges of computational complexity on resource-limited terminal devices. In addition, [25] adopted a compression technique in their scheme, which focuses on compressing the access policy in CP-ABE by leveraging the repetitive nature of attribute sets. However, the reduction in ciphertext size using this technique is limited due to the limited occurrence of repetitive data within the access policy. Another scheme proposed by [26] addressing the inefficiencies and limitations of previous threshold attribute-based encryption (ABE) schemes. The proposed scheme allows for flexible attribute selection and threshold values, making it practical for real-world applications. such as access control in Massively Multiplayer Online Games (MMOGs). However, the proposed scheme is designed specifically for threshold ABE, which may limit its applicability in other scenarios that require different access control mechanisms.

Hence, addressing the issue of ciphertext size is crucial for the widespread adoption and practical implementation of CP-ABE. By reducing the size of ciphertexts, the overall efficiency of the system can be enhanced, enabling faster encryption and decryption operations and reducing resource consumption. Additionally, smaller ciphertexts contribute to improved data transmission and storage efficiency, making CP-ABE more suitable for real-world applications.

4.2. Multi-Authority Architecture

Multi-Authority refers to an architecture where multiple attribute authorities collaborate to manage and enforce access control policies. In this setup, each authority has the responsibility of issuing attributes and managing associated user access policies. Multi-Authority CP-ABE extends the capabilities of traditional CP-ABE by distributing the authority and management of attributes among multiple entities. For cloud systems, multi-authority is more practical and secure because it does not rely on a single authority. Nevertheless, there are several problems with multi-authority that researchers need to address. First, users may join or leave the system dynamically, requiring corresponding changes to their authorizations. Second, in practical applications, attributes may need to be added or revoked. The public parameters of the system depend on the attribute universe, which is fixed when the system is initialized. Multi-authority aims to increase efficiency and practicality compared to single-authority systems, which are more prone to failure. In multi-authority, multiple authorities are enabled to oversee user attributes and distribute secret keys while being resilient to corruption among the authorities. Nonetheless, the effectiveness of the decryption process will diminish as the number of users increases.

Several approaches have been developed to address the issue in multi-authority in CP-ABE. One notable approach is the threshold-based key generation approach (TKGA) proposed by [27], which aims to enhance security by preventing collusion attacks. [28] introduce a different approach that enables multiple authorities to manage key issuance for an exponential number of attributes without the need for prior specification, utilizing prime order bilinear groups.

In contrast, the researchers in [29] focus on achieving attribute-based encryption with fast decryption in multi-authority systems. They implement this by leveraging fast decryption techniques and employing logical operations such as AND, OR, and threshold policies. Additionally, [30] introduces a decentralized multi-authority ciphertext-policy attribute-based encryption (DCP-ABE) scheme. This scheme enables any party to act as an authority by generating public and private keys for users based on their attributes. Both approaches significantly advance the development of multi-authority systems in attribute-based encryption, each offering unique features and contributions. Their research efforts aim to improve the security, efficiency, and practicality of multi-authority ABE schemes, thereby supporting the implementation of secure and flexible access control mechanisms in cloud environments.

4.3. Users Revocation

Revocation is a crucial aspect of CP-ABE systems, involving the removal or revocation of access privileges or attributes granted to users. Attribute-based revocation allows for precise control over access privileges, ensuring that revoked users no longer have decryption capabilities for protected data. Revocation can be implemented through online or offline methods, with online revocation enabling real-time access revocation and offline revocation facilitating periodic updates. Techniques such as attribute revocation lists (ARLs), time-limited attributes, and threshold schemes have been proposed to ensure efficient and scalable revocation in CP-ABE. Efficient key update and distribution mechanisms are essential for reflecting attribute revocation in users' decryption keys while minimizing computational and communication overhead. Balancing security, efficiency, and system complexity, revocation in CP-ABE involves trade-offs that researchers continuously explore to enhance the effectiveness and efficiency of revocation mechanisms.

In practical applications of CP-ABE, the challenge lies in revoking the secret key of a user who no longer possesses access privileges. Forward secrecy and collusion-resistance are two crucial security properties that follow user revocation. Achieving forward secrecy ensures that revoked users cannot decrypt any ciphertext. However, re-encrypting data for all revoked users can be impractical, especially in large companies with a vast amount of data. Additionally, updating encryption processes becomes complex when encryptors are unavailable during attribute and access policy updates. To address these challenges, researchers have proposed solutions. For example, [31] introduced CP-ABE with supporting Access Policy Update (CP-ABE-APU), which facilitates revocation and access policy updates. [32] employed a dynamic binary tree instead of a static binary tree to enhance system scalability and address revocation challenges.

Authors in [33] proposes a novel CP-ABE scheme that supports updatable capabilities while incorporating white-box traceability and traitor revocation. The scheme introduces a "fixed point" embedded within the user's secret key to enable traceability, and each user is assigned a unique identifier for revocation purposes. Additionally, the secret exponent used for message encryption is divided into two parts: one for the access policy and the other for the revocation list. This division allows for updating only a portion of the ciphertext components when the revocation list changes, simplifying the ciphertext update process. However, the use of the revocation list in this scheme have resulted in increased ciphertext size, posing potential challenges in terms of high storage costs.

Authors [34] proposed a secure access control scheme for collaborative eHealth systems, aiming to enable the secure sharing of health data while ensuring immediate attribute/user revocation and achieving forward and backward security. The scheme employs an access structure based on ordered binary decision diagrams (OBDD) and associates user keys with user identities to realize these features. However, the proposed scheme faces feasibility challenges. The ciphertext and key sizes increase linearly with the number of attributes involved, which can be problematic in environments with numerous attributes but limited storage and network resources. Moreover, the computational efficiency of the scheme may experience a slight decrease depending on the size of the real health data being protected when implemented in real-world scenarios.

Meanwhile, works by [35] proposed a CP-ABE scheme that incorporates revocation, white-box traceability, and the application of partially hidden policies. The scheme divides the ciphertext into two parts: one related to the access policy, encrypted using attribute values where only the attribute names are evident, and the other related to revocation information. The revocation information is updated when revocations occur and is generated through a binary tree associated with users. The leaf node value in the decryption key's binary tree is utilized for tracing malicious users. While this scheme allows for the detection of malicious users, it is insufficient as the access policy is vulnerable to privacy leakage, and there is a possibility for the ciphertext size to increase significantly.

In summary, all the studies have focused on attribute revocation schemes in user collision avoidance systems. These schemes incorporate concepts like white-box traceability, traitor revocation, and partially hidden policies. Their primary objective is to facilitate secure data sharing while ensuring traceability and revocation capabilities. However, some of these schemes encounter challenges such as increased ciphertext size and the potential for privacy leakage in access policies. Therefore, revocation in CP-ABE systems necessitates careful consideration of security, efficiency, and practical feasibility. Researchers continue to explore innovative approaches and optimizations to enhance revocation mechanisms, ultimately enabling the secure and efficient sharing of sensitive data across various domains.

4.4. Access Policy Hiding

The access policy defined for the encrypted message is often sent in unencrypted format in classical ABE. It allows unauthorized parties to get attribute details from the access policy and then disclose the information. As a result, numerous scholars [14][36][37] developed novel ABE systems. The authors introduce the CP-ABE in [36] which intends to manage data accessing over the Cloud via access policy. [37-38] also proposes CP-ABE as a way to improve the efficiency of data sharing between data owners and other consumers. It also allowed data owners to set an encryption data access policy, allowing only people who met the criteria to download and reveal the data.

Works by [39] highlights that numerous proposed CP-ABE schemes have successfully met their objectives by facilitating efficient and secure data sharing. However, many of these frameworks have neglected the privacy concerns of data owners and users. For example, consider a scenario depicted in Figure 3 where a Data Owner encrypts a health record with an access policy A= ((Affiliation: City Hospital AND Department: Respiratory) OR (SSN: 32154-6789 AND Status: Normal)), and the ciphertext is stored with the CSP. In this situation, anyone, including the CSP, can view the access policy and potentially infer that the user with Social Security number 321-54-6789 may have a respiratory issue. This leads to a breach in the user's privacy, underscoring the importance of concealing the access policy. Therefore, it's crucial to implement an encryption strategy that not only secures the data during transmission but also completely obscures the details within the access policy.

In CP-ABE scheme, the ciphertext is merged with an access policy and it will be outsourced to the Cloud. The access policy contain is an access formula which implemented using an access tree, generated by a set of Boolean formulas demonstrating attributes of a user. The access tree can consist of different types, such as AND gates and threshold gates, where non-leaf nodes are defined by threshold values. The owner transmits the access policy along with the ciphertext, and it is essential to hide the access formula in order to prevent unauthorized access and protect sensitive data.

Previous CP-ABE schemes did not hide the access policy, allowing hackers to learn the access formula and attributes, leading to potential security breaches. To overcome this limitation, researchers have proposed new schemes that focus on hiding access policies. For example, [41] proposed a scheme where users keep the access policies with information in encrypted form, utilizing composite order bilinear groups. [42] expanded the technique using AND gates with wildcards to achieve hidden access policies. [43] presented a secure CP-ABE scheme using composite-order bilinear groups that hide the access policy. An effective and trustworthy CP-ABE scheme with hidden policies was introduced by [44]. By employing the dual system encryption methods, they make sure their plan is fully secure under the assumption of static data. This method maintains a small ciphertext size while supporting AND gates with negative, positive, and wildcard access policies. In order to prevent receivers from the ciphertext, [45] suggested a searchable CP-ABE technique with attribute revocation and hidden access policy.

In a separate study, [37] put forward a method for hidden access policy with fast decryption. Their approach involved transmitting the mapping function rather than the actual attribute value of the access policy. However, this decision to use the mapping function introduced a privacy vulnerability as it indirectly revealed information about the attribute value. Therefore, if the mapping function were to be exposed, it could be exploited by malicious individuals to reconstruct the access policy.

Furthermore, the researchers implemented constant bilinear pairing to enable fast decryption. However, this scheme encountered a drawback in terms of high storage cost due to the increase in ciphertext size associated with the access policy. Researchers in [46] introduced a policy-hiding CP-ABE framework designed to offer a fine-grained data access control scheme suitable for cloud-based IoT, featuring an expressive access policy with fully hidden attributes. Their approach utilizes a randomizable technique to ensure complete concealment of the access policy. Additionally, they developed a fuzzy attribute positioning mechanism using a garbled Bloom filter, aiding authorized recipients in efficiently locating their attributes and successfully decrypting the ciphertext. However, in their experiments, they primarily focused on simulating the encryption and decryption algorithms using four elliptic curves, without conducting an in-depth performance analysis of the scheme.

Conversely, reference [47] proposed an efficient policy-hiding attribute-based scheme integrated with keyword search functionality for Cloud-assisted IoT systems. This scheme, built on a prime order group, is both secure and practical for real-world implementation. However, it is important to note that this scheme is restricted to static data, limiting its applicability in dynamic environments.

Recently, many researchers have proposed solutions to address the limitations of existing CP-ABE schemes. For example, the authors in [48] introduced a multi-authority CP-ABE scheme (RMA-CPABE) designed to protect user privacy through access policy hiding. Specifically tailored for fog-enabled IoT environments, this scheme effectively handles user revocation and optimizes performance for resource-constrained devices. Instead of tying ciphertext size to the number of attributes, it relates it to the number of domain authorities, which significantly reduces ciphertext overhead. The model also supports attribute updates and outsourced decryption, thereby minimizing the computational burden on end-user devices. A key strength of RMA-CPABE is that it avoids the need for complex ciphertext updates during attribute revocation or addition—an issue common in many existing schemes. It ensures secure access using constant-size user keys and is proven to be secure against Chosen-Ciphertext Attacks (CCA). Performance evaluations suggest it is well-suited for practical IoT applications.

Similarly, works by [49][50] present advanced CP-ABE schemes aimed at enhancing secure data sharing in IoT environments, though they target different use cases. The FOC-PH-CP-ABE scheme is designed for Industrial IoT, where devices often have limited processing capabilities. It leverages fog computing to fully outsource encryption, and decryption processes and includes efficient mechanisms for both user and attribute revocation—without imposing significant overhead. The scheme also boasts strong security, formally proven under the q-BDHE assumption. In contrast, the scheme [49] is suited for more dynamic 5G-enabled IoT scenarios, where user groups frequently change. It employs the Chinese Remainder Theorem (CRT) for lightweight group key management, ensures policy hiding through attribute obfuscation, and incorporates collusion resistance by binding group and attribute keys. While FOC-PH-CP-ABE [50] is ideal for centralized, stable environments that require robust access control and performance efficiency, MGPH-ABE excels in flexible, fast-changing contexts. However, MGPH-ABE's reliance on cloud-edge collaboration may introduce latency or synchronization issues, whereas FOC-PH-CP-ABE may struggle to scale in highly dynamic environments. Overall, each scheme presents a strong, context-specific solution for enhancing data security and access control in modern IoT ecosystems.

5. CONCLUSION

In conclusion, this research provides a comprehensive examination of Ciphertext Policy Attribute-Based Encryption (CP-ABE) in cloud storage. It identifies and analyzes key implementation challenges, such as attribute revocation, access policy obfuscation, ciphertext size, and multi-authority concerns. The study delves into these issues and areas of focus among CP-ABE researchers, elucidating the solutions and developments proposed by leading contributors in the field. The findings underscore the need for continuous improvement and innovation in CP-ABE to address evolving security demands in cloud storage, providing valuable insights for both academic researchers and industry practitioners. This paper contributes significantly to the field, advancing the understanding of secure cloud computing and offering practical insights for enhancing data security in cloud environments.

Acknowledgements

This research was funded by a grant from Universiti Sultan Zainal Abidin through Center for Research Excellence and Incubation Management (CREIM) (UniSZA/2023/DPU1.0/07).

REFERENCES

[1] V. Chang, Y. H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Future Generation Computer Systems, vol. 57, pp. 24-41, 2016.

[2] T. Mahboob, Z. Maryam, and A. Gulnoor, "Adopting Information Security Techniques for Cloud Computing - A Survey," Proceedings of the 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2016, pp. 7-11, Institute of Electrical and Electronics Engineers Inc., 2016.

[3] X. Sun, "Critical Security Issues in Cloud Computing: A Survey," Proceedings of the 4th IEEE International Conference on Big Data Security on Cloud, Big DataS ecurity 2018, 4th IEEE International Conference on High Performance and Smart Computing, HPSC 2018, and 3rd IEEE International Conference on Intelligent Data and Security, pp. 216-221, 2018.

[4] B. Lokesh Bhajantri and M. Tabassum, "A Survey of Cloud Computing Security Challenges, Issues and Their Countermeasures," Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019, pp. 376-380, 2019

[5] J. Pan Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions," IEEE Access, vol. 7, pp. 147420-147452, 2019.

[6] E. Sibai, G. Rayane, G. Nader, A. Bou Jacques, and D. Jacques, "A Survey on Access Control Mechanisms for Cloud Computing," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 2, 2020.

[7] B. Seth, S. Dalal, V. Jaglan, D. Nhuong Le, S. Mohan, and G. Srivastava, "Integrating Encryption Techniques for Secure Data Storage in the Cloud," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 4, 2022.

[8] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, N. Javed, M. Alam, and F. Jamil, "A Survey of Cloud Computing Data Integrity Schemes: Design Challenges, Taxonomy and Future Trends," Computers and Security, vol. 65, pp. 29-49, March 2017.

[9] A. R. Khan, "Access Control in Cloud Computing Environment," ARPN Journal of Engineering and Applied Sciences, vol. 7, no. 5, pp. 613-615, 2012.

[10] G. Revathy, P. M. Priya, R. Saranya, and C. Ramchandran, "Cloud Storage and Authenticated Access for Intelligent Medical System," Proceedings of the 6th International Conference on Computing Methodologies and Communication, ICCMC 2022, pp. 53-56, 2022. Institute of Electrical and Electronics Engineers Inc.

[11] S. M. P. C. Souza, and R. S. Puttini, "Client-Side Encryption for Privacy-Sensitive Applications on the Cloud," Procedia Computer Science, vol. 97, pp. 126–30, 2016.

[12] X. Niu, "Fine-Grained Access Control Scheme Based on Cloud Storage," in Proceedings - 2017 International Conference on Computer Network, Electronic and Automation, ICCNEA 2017, Institute of Electrical and Electronics Engineers Inc, pp. 512–15, 2017.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in CCS '06: Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98, 2006.

[14] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” in 2007 IEEE Symposium on Security and Privacy (SP ’07), 2007, pp. 321–34, 2007.

[15] N. Chen, J. Li, Y. Zhang, and Y. Guo, “Efficient CP-ABE Scheme with Shared Decryption in Cloud Storage,” IEEE Transactions on Computers, vol. 71, no. 1, pp. 175–84, 2022.

[16] C. Li, J. He, C. Lei, C. Guo, and K. Zhou, “Achieving Privacy-Preserving CP-ABE Access Control with Multi-Cloud,” in 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications, pp. 801–8, 2019.

[17] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, “TrustAccess: A Trustworthy Secure Ciphertext-Policy and Attribute Hiding Access Control Scheme Based on Blockchain,” IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5784–98, 2020.

[18] P. Chinnasamy, P. Deepalakshmi, A. K. Dutta, J. You, and G. P. Joshi, “Ciphertext-Policy Attribute-Based Encryption for Cloud Storage: Toward Data Privacy and Authentication in Ai-Enabled IoT System,” Mathematics, vol. 10, no. 1, 2022.

[19] Y. Li, J. Zhu, X. Wang, Y. Chai, and S. Shao, “Optimized Ciphertext-Policy Attribute-Based Encryption with Efficient Revocation,” International Journal of Security and Its Applications, vol. 7, no. 6, pp. 385–94, 2013.

[20] K. Sethi, A. Pradhan, and P. Bera, “Practical Traceable Multi-Authority CP-ABE with Outsourcing Decryption and Access Policy Updation,” Journal of Information Security and Applications, vol. 51, p. 102435, 2020.

[21] R. Zhang, H. Ma, and Y. Lu, “Fine-Grained Access Control System Based on Fully Outsourced Attribute-Based Encryption,” Journal of Systems and Software, vol. 125, pp. 344–53, 2017.

[22] X. Liu, H. Wang, B. Zhang, and B. Zhang, “An Efficient Fine-Grained Data Access Control System with a Bounded Service Number,” Information Sciences, vol. 584, pp. 536–63, 2022.

[23] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, and K. K. R. Choo, “Pairing-Based CP-ABE with Constant-Size Ciphertexts and Secret Keys for Cloud Environment.” Computer Standards and Interfaces. 54 (November): 3–9, 2017.

[24] X. Li, T. Liu, C. Chen, Q. Cheng, X. Zhang, and N. Kumar, “A Lightweight and Verifiable Access Control Scheme With Constant Size Ciphertext in Edge-Computing-Assisted IoT,” IEEE Internet of Things Journal, vol. 9, no. 19, pp. 19227–19237, 2022.

[25] Z. Zhang, C. Li, B. B. Gupta, and D. Niu, “Efficient Compressed Ciphertext Length Scheme Using Multi-Authority CP-ABE for Hierarchical Attributes,” IEEE Access, vol. 6, pp. 38273–38284, 2018

[26] W. Susilo, G. Yang, F. Guo, and Q. Huang, “Constant-Size Ciphertexts in Threshold Attribute-Based Encryption without Dummy Attributes,” Information Sciences, vol. 429, pp. 349–360, 2018.

[27] W.-B. Huang, W.-T. Su, and C.-S. Liang, “A Threshold-Based Key Generation Approach for Ciphertext-Policy Attribute-Based Encryption,” in 2015 Seventh International Conference on Ubiquitous and Future Networks, pp. 908-913, 2015.

[28] Y. Rouselakis and B. Waters, “Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption,” Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8975, pp. 315–332, 2015.

[29] N. Gorasia, R. R. Srikanth, N. Doshi, and J. Rupareliya, “Improving Security in Multi Authority Attribute Based Encryption with Fast Decryption,” Procedia Computer Science, vol. 79, pp. 632–639, 2016.

[30] M. S. Rahman, A. Basu, and S. Kiyomoto, “Decentralized Ciphertext-Policy Attribute-Based Encryption from Learning with Errors over Rings,” in 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 1759–1764, 2016.

[31] Y. Jiang, W. Susilo, Y. Mu, and F. Guo, “Ciphertext-Policy Attribute Based Encryption Supporting Access Policy Update,” Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10005 LNCS, pp. 39–60, 2016.

[32] N. Vaanchig, W. Chen, and Z. Qin, “Ciphertext-Policy Attribute-Based Access Control with Effective User Revocation for Cloud Data Sharing System,” in 2016 International Conference on Advanced Cloud and Big Data (CBD), pp. 186–193, 2016.

[33] Z. Liu, J. Xu, Y. Liu, and B. Wang, “Updatable Ciphertext-Policy Attribute-Based Encryption Scheme with Traceability and Revocability,” IEEE Access, vol. 7, pp. 66832–66844, 2019.

[34] K. Edemacu, B. Jang, and J. W. Kim, “Collaborative Ehealth Privacy and Security: An Access Control with Attribute Revocation Based on OBDD Access Structure,” IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 10, pp. 2960–2972, 2020.

[35] D. Han, N. Pan, and K. C. Li, “A Traceable and Revocable Ciphertext-Policy Attribute-Based Encryption Scheme Based on Privacy Protection,” IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 316–327, 2022.

[36] X. Liu, Y. Xia, W. Yang, and F. Yang, “Secure and Efficient Querying over Personal Health Records in Cloud Computing,” Neurocomputing, vol. 274, pp. 99–105, Jan. 2018.

[37] 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.

[38] S. Sabitha and M. S. Rajasree, “Access Control Based Privacy Preserving Secure Data Sharing with Hidden Access Policies in Cloud,” Journal of Systems Architecture, vol. 75, pp. 50–58, 2017.

[39] G. Ramachandra, M. Iftikhar, and F. A. Khan, “A Comprehensive Survey on Security in Cloud Computing,” Procedia Computer Science, vol. 110, pp. 465–472, 2017.

[40] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, “Attribute-Based Encryption for Cloud Computing Access Control: A Survey,” ACM Computing Surveys, Association for Computing Machinery, 2020.

[41] U. C. Yadav, “Ciphertext-Policy Attribute-Based Encryption with Hiding Access Structure,” in 2015 IEEE International Advance Computing Conference (IACC), pp. 6–10, 2015.

[42] T. V. X. Phuong, G. Yang, and W. Susilo, “Hidden Ciphertext Policy Attribute-Based Encryption under Standard Assumptions,” IEEE Transactions on Information Forensics and Security, vol. 11, pp. 35–45, 2016.

[43] U. C. Yadav and S. T. Ali, “Ciphertext Policy-Hiding Attribute-Based Encryption,” in 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2067–2071, 2015.

[44] C. Jin, X. Feng, and Q. Shen, “Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size,” in ACM International Conference Proceeding Series, pp. 88–95, 2016.

[45] J. Li, Y. Shi, and Y. Zhang, “Searchable Ciphertext-Policy Attribute-Based Encryption with Revocation in Cloud Storage,” International Journal of Communication Systems, vol. 30, no. 1, 2017.

[46] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, and X. (S.) Shen, “Fine-Grained Data Access Control with Attribute-Hiding Policy for Cloud-Based IoT,” Computer Networks, vol. 153, pp. 1–10, 2019.

[47] H. Yin, Y. Li, F. Li, H. Deng, W. Zhang, and K. Li, “An Efficient and Access Policy-Hiding Keyword Search and Data Sharing Scheme in Cloud-Assisted IoT,” Journal of Systems Architecture, vol. 128, July 2022.

[48] C. K. Chaudhary, R. Sarma, and F. A. Barbhuiya, “RMA-CPABE: A Multi-Authority CPABE Scheme with Reduced Ciphertext Size for IoT Devices,” Future Generation Computer Systems, vol. 138, pp. 226–242, 2023.

[49] Luo, W., Lv, Z., Yang, L., Han, G., & Zhang, X. (2024). FOC-PH-CP-ABE: an efficient CP-ABE scheme with fully outsourced computation and policy-hidden in the Industrial Internet of Things. IEEE Sensors Journal

[50] Cai, J., Zhang, H., Duo, Z., Wang, X., & Zhao, X. (2024). A Multi-Group-Supporting Policy Hidden Fine-Grained Data Sharing Scheme in 5G-Enabled IoT with Edge Computing. IEEE Access.

Authors

	Siti Dhalila Mohd Satar received her Ph.D. from Universiti Putra Malaysia in 2024 and her M.Sc. from Universiti Teknologi Malaysia in 2012. She is a Lecturer at Universiti Sultan Zainal Abidin, specializing in access control security systems, security services—including digital forensics, steganography, network security, and biometrics—and data security. Her research contributions focus on advancing security mechanisms to protect digital ecosystems.
	Masnida Hussin Dr. Masnida Hussin is an Associate Professor (Ts. Dr.) at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). She holds a Ph.D. in Computer Science from the University of Sydney, Australia (2012), a Master of Science in Computer Science from UPM (2006), and a Bachelor of Science from Universiti Teknologi Malaysia (UTM). Her research interests include cloud computing, distributed systems, virtualization, energy-efficient computing, and high-performance computing. She has made significant contributions to areas such as resource allocation, load balancing, and security within cloud and fog computing environments. She can be contacted via email at: **masnida@upm.edu.my**.

	Nazirah Abd Hamid is a senior lecturer in University Sultan Zainal Abidin, Terengganu, Malaysia. She holds a degree in Bachelor of Information Technology from University Utara Malaysia (UUM), in 2004, M. Sc. Com. (Information Security) from University Teknologi Malaysia (UTM), in 2011 and PhD in Computer Science from Universiti Teknikal Malaysia Melaka (UTeM), in 2023. Her research interests are Information Security, Cyber Security, Pattern Recognition and Data Mining. She can be contacted at email: nazirah@unisza.edu.my.
	Mohamad Afendee Mohamed received his Ph.D. in Mathematical Cryptography from Universiti Putra Malaysia in 2011. Upon completion, he served the university for three years as a senior lecturer. In 2014, he moved to Universiti Sultan Zainal Abidin and later assumed an associate professor position. His current research interests include both theoretical and application issues in the domain of data security and mobile and wireless networking. He has authored more than 100 articles that have appeared in various journals, book chapters, and conference proceedings. He can be contacted at email: mafendee@unisza.edu.my.