PERFORMANCE OPTIMIZATION OF CLOUD STORAGE IN ACCESS CONTROL OF CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION

By

SITI DHALILA BINTI MOHD SATAR

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

November 2023

FSKTM 2023 12

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

PERFORMANCE OPTIMIZATION OF CLOUD STORAGE IN ACCESS CONTROL OF CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION

By

SITI DHALILA BINTI MOHD SATAR

November 2023

Chair : Associate Professor Masnida Binti Hussin, PhD
Faculty : Computer Science and Information Technology

In this research, we address the critical need for enhanced cloud computing security and performance by developing an access control framework. This framework integrates an Ciphertext Policy Attribute-based Encryption (CP-ABE) with mechanisms aimed at optimizing the performance of access policy hiding process while strengthening the users' privacy and streamlining data access processes. Specifically, we introduce a modified CP-ABE model that incorporates Access Policy Hiding (APH), the Tokenization Identifier (TId) technique, and Priority Task Scheduling (PriTask) to tackle prevalent challenges in cloud storage systems.

The core of our proposal lies in the implementation of APH to optimize the performance of concealing access policies, a move that significantly curtails potential privacy breaches by preventing unauthorized entities from gleaning attribute information from access policies. This strategy not only enhances user privacy but also contributes to a reduction in processing time which increase the performance of CP-ABE. Concurrently, the TId technique is employed to mitigate data redundancy within files. This method ensures a more compact plaintext format, thereby reducing the storage cost, optimizing the performance of encryption and minimizing the demands on cloud storage space. To address the inefficiencies during peak traffic periods, our framework incorporates the PriTask module, a scheduling mechanism designed to prioritize decryption tasks. This optimization reduces response times and average delay time, ensuring swift and reliable access to encrypted data stored in the cloud.

Our experimental setup utilized a CP-ABE simulation tool, developed using Java and leveraging the CP-ABE open-source library, with foundational support from the Java pairing-based cryptography (JPBC) library. The empirical evidence highlights the efficacy of our approach, revealing a 10.6% improvement in

average processing time—679 milliseconds compared to the benchmark of 791 milliseconds. Moreover, our method achieved a nearly 5% reduction in storage cost relative to standard models. The introduction of PriTask notably expedited decryption processes and alleviated response times, further underscoring the performance advantages of our modified CP-ABE framework.

In summary, the integration of APH, TId, and PriTask within a modified CP-ABE schema presents a robust solution to the dual challenges of cloud security and data access efficiency. This study not only demonstrates the feasibility of enhancing cloud data management through innovative encryption and scheduling techniques but also sets the stage for future research avenues, including advanced attribute management, multi-tiered access control, and scalability enhancements. Our findings contribute to the ongoing evolution of secure and efficient cloud computing paradigms.

Keywords: Access Control, Ciphertext Policy Attribute based Encryption, Cloud Storage, Performance Optimization

SDG: GOAL 9: Industry, Innovation and Infrastructure

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENGOPTIMUMAN PRESTASI PENYIMPANAN AWAN DALAM KAWALAN AKSES PENYULITAN BERASASKAN ATRIBUT POLISI TEKS SIFER

Oleh

SITI DHALILA BINTI MOHD SATAR

November 2023

Pengerusi : Profesor Madya Masnida Binti Hussin, PhD
Fakulti : Sains Komputer dan Teknolologi Maklumat

Dalam kajian ini, kami menangani keperluan penting untuk meningkatkan keselamatan dan prestasi pengkomputeran awan dengan membangunkan satu kerangka kawalan akses. Kerangka ini mengintegrasikan Penyulitan Berasaskan Atribut Polisi Teks Sifer (CP-ABE) dengan mekanisme yang bertujuan untuk mengoptimumkan prestasi proses penyembunyian dasar akses sambil menguatkan privasi pengguna dan memperkemas proses akses data. Secara khusus, kami memperkenalkan model CP-ABE yang diubahsuai yang merangkumi Penyembunyian Dasar Akses (APH), teknik Pengenalpastian Tokenisasi (TId), dan Penjadualan Tugas Keutamaan (PriTask) untuk menangani cabaran yang lazim dalam sistem penyimpanan awan.

Cadangan utama kami terletak pada pelaksanaan APH untuk mengoptimumkan prestasi menyembunyikan dasar akses, langkah yang secara signifikan mengurangkan potensi pelanggaran privasi dengan menghalang entiti yang tidak sah mendapatkan maklumat atribut dari polisi akses. Strategi ini tidak hanya meningkatkan privasi pengguna tetapi juga menyumbang kepada pengurangan masa pemprosesan yang meningkatkan prestasi CP-ABE. Secara serentak, teknik TId digunakan untuk mengurangkan data berulang dalam fail. Kaedah ini memastikan format teks biasa yang lebih padat, dengan itu mengurangkan kos penyimpanan, mengoptimumkan prestasi penyulitan dan meminimumkan permintaan pada ruang penyimpanan awan. Untuk menangani ketidakefisienan semasa tempoh trafik puncak, kerangka kami memasukkan modul PriTask, mekanisme penjadualan yang direka untuk memberi keutamaan kepada tugas-tugas dekripsi. Pengoptimuman ini mengurangkan masa tindak balas dan masa kelewatan purata, memastikan akses yang cepat dan boleh dipercayai kepada data yang disulitkan yang disimpan dalam awan.

Untuk menangani ketidakcukupan semasa tempoh trafik puncak, kerangka kerja kami menggabungkan modul PriTask, mekanisme penjadualan yang direka untuk memberi keutamaan kepada tugas-tugas dekripsi. Pengoptimuman ini mengurangkan masa respons dan kelewatan dekripsi, memastikan akses yang cepat dan boleh dipercayai kepada data yang disulitkan yang disimpan dalam awan.

Penyediaan eksperimen kami menggunakan alat simulasi CP-ABE, yang dibuat menggunakan Java dan memanfaatkan perpustakaan sumber terbuka CP-ABE, dengan sokongan asas dari perpustakaan kriptografi berpasangan berasaskan Java (JPBC). Bukti empirikal menonjolkan keberkesanan pendekatan kami, mendedahkan peningkatan purata masa pemprosesan sebanyak 10.6%—679 milisaat berbanding dengan kajian rujukan sebanyak 791 milisaat. Selain itu, kaedah kami mencapai pengurangan hampir 5% dalam kos penyimpanan berbanding dengan model standard. Pengenalan PriTask secara ketara mempercepat proses dekripsi dan mengurangkan masa tindak balas, lebih menekankan lagi kelebihan prestasi kerangka CP-ABE yang telah diubahsuai.

Secara ringkas, integrasi APH, TId, dan PriTask dalam skema CP-ABE yang dimodifikasi menyajikan penyelesaian yang kuat kepada cabaran ganda keselamatan awan dan kecekapan akses data. Kajian ini tidak hanya menunjukkan kebolehlaksanaan meningkatkan pengurusan data awan melalui teknik penyulitan dan penjadualan yang inovatif tetapi juga menetapkan pentas untuk lorong penyelidikan masa depan, termasuk pengurusan atribut lanjutan, kawalan akses berbilang tingkat, dan peningkatan kebolehskalaan. Penemuan kami menyumbang kepada evolusi berterusan paradigma pengkomputeran awan yang selamat dan efisien.

Kata Kunci: Kawalan Akses, Pengoptimuman Prestasi, Penyimpanan Awan, Penyulitan Berasaskan Atribut Polisi Teks Sifer

SDG: GOAL 9: Industry, Innovation and Infrastructure

ACKNOWLEDGEMENTS

First and foremost, I would like to express my profound gratitude to Allah Subhanahu Wa Taala for endowing me with the courage, strength, guidance, patience, and the opportunity to successfully complete this transformative PhD journey. Throughout every stage of my life, I have been accompanied by His boundless mercy and blessings, for which I am deeply thankful. May blessings and peace be upon Prophet Muhammad Sallalahu Alaihi Wasallam, who was sent as a wellspring of mercy to the entire world.

I extend my heartfelt appreciation to my supervisor, Associate Professor Dr. Masnida Hussin. Her professional guidance and counsel have been invaluable companions throughout my PhD journey. Her profound knowledge, especially within the research domain, has significantly influenced my research. I am truly indebted for the way she has shaped my academic growth. Thank you, Dr. Masnida!

Grateful acknowledgments extend to my supervisory committee members: Associate Professor Dr. Zurina Mohd Hanapi and Associate Professor Dr. Afendee Mohamed. Their thoughtful comments and insightful suggestions have enriched this journey. Our discussions during progress presentations have been enlightening, providing perspectives and recommendations that have elevated my understanding and realization of this work.

Lastly, my heart brims with gratitude towards my family for their unwavering prayers and unending encouragement. A special acknowledgment is reserved for my husband, Mohd Najib Bin Alias, whose unwavering support has been my rock. To my children, Damia, Dhiya, and Nuqman, your love and concern have been my wellspring of strength. I deeply appreciate your understanding and patience.

To all my friends, your continued understanding has been a constant source of inspiration. To those whose names are too numerous to mention, without your support, all these would not be possible.

I thank Allah truly for these blessings.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Masnida binti Hussin, PhD
Associate Professor Ts.
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zurina binti Md Hanapi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Mohamad Affendee bin Mohamed, PhD
Associate Professor
Faculty of Informatics and Computing
Universiti Sultan Zainal Abidin
(Member)

_____
ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 11 July 2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CP-ABE	Ciphertext Policy Attribute-based Encryption
APH	Access Policy Hiding
TId	Tokenization Identifier
PriTask	Priority Task Scheduling
GPBC	Java Pairing-based Cryptography
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
AWS	Amazon Web Services
CRM	Customer Relationship Management
CC	Cloud computing
CSP	Cloud Services Providers
ABE	Attribute-based Encryption
RP	Research Problems
RQ	Research Questions
RO	Research Objectives
RC	Research Contribution
NIST	National Institute of Standards and Technology
CIA	Confidentiality, Integrity and Availability
DAC	Discretionary Access Control
MAC	Mandatory Access Control
RBAC	Role Based Access Control
ACL	Access Control List
ABAC	Attribute-Based Access Control

KP-ABE	Key-Policy Attribute-based Encryption
DO	Data Owner
AES	Advanced Encryption Standard
TKGA	Threshold-based Key Generation Approach
DCP-ABE	Decentralized Ciphertext Policy Attribute-based Encryption
WMN	Wireless Mesh Networks
ARL	Attribute Revocation Lists
EHR	Electronic Health Record
ODBD	Ordered Binary Decision Diagram
LSSS	Linear Secret Sharing Scheme
DU	Data User
AA	Attribute Authority
GHz	Gigahertz
GB	Gigabyte
RAM	Random Access Memory
CT	Ciphertext
ExAPH	Extraction of Access Policy Hiding
HV	Hidden Value
FCFS	First Come First Serve
HPQ	High Priority Queue
LPQ	Low Priority Queue
Kb	Kilobyte
ms	Milisecond

CHAPTER 1

INTRODUCTION

Cloud computing has revolutionized the digital information landscape by offering a wide array of IT resources (Figure 1.1). The spectrum of cloud services includes Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS provides users with application access such as webmail and web browsers, PaaS delivers development tools like programming languages and libraries, and IaaS offers fundamental resources like storage, networks, and computing power.

The deployment models of cloud computing are categorized into private, public, community, and hybrid clouds. Each deployment model caters to specific organizational needs and security considerations. A private cloud is exclusive to a single organization, ensuring dedicated resources and security, for example, for sensitive data and internal communications. In contrast, a public cloud is available to multiple users and organizations, offering scalability and cost-effectiveness, exemplified by services like Amazon Web Services (AWS). A community cloud serves a specific group with common interests or requirements, such as government agencies sharing resources for cost-efficiency and specialized services. Finally, a hybrid cloud combines elements of private, public, and community clouds, providing versatility and tailored solutions; for instance, a business might use a private cloud for secure data and a public cloud for high-demand services like customer relationship management (CRM) software. These models enable users to choose services and deployment strategies that best fit their unique needs and constraints, as discussed in the works of Kajiyama et al. (2017), Mell et al. (2015), Ramachandra et al. (2017), Rimal et al. (2009), and Rong et al. (2019).

Cloud computing, adopted across various sectors like business, military, and healthcare, significantly enhance the operations by providing on-demand services like storage, computation, and data sharing. The pay-per-use model facilitates seamless, geographically unrestricted data sharing, thereby reducing management costs and enhancing organizational performance and client satisfaction. This trend is highlighted in studies by Tweneboah-Koduah et al. (2014), Abied et al. (2022), Adjei (2015), and Nanos et al. (2019).

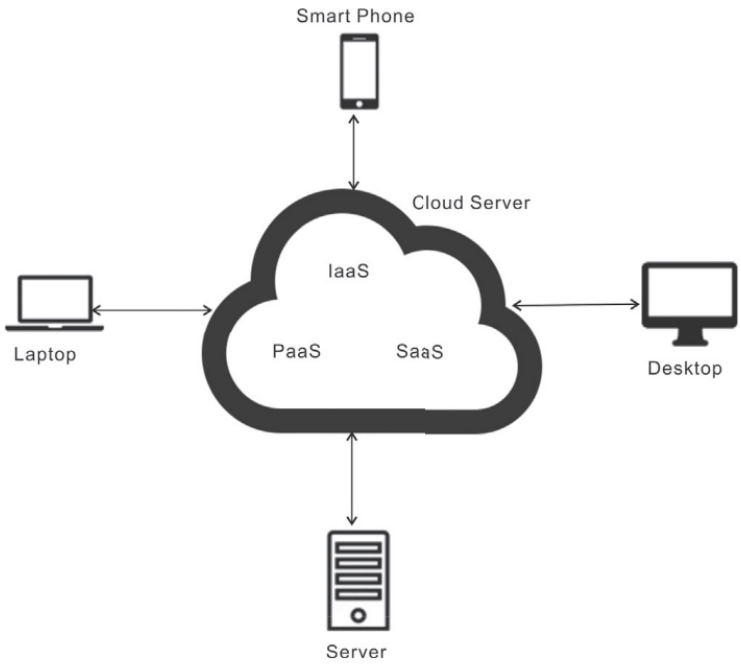

Figure 1.1: Cloud Computing Architecture
(Source Kumar & Alphonse, 2018)

With the ease of access to Cloud services and countless benefits, organizations are gearing up to use Cloud computing in their business operations and management. One of the areas that organizations notoriously prefer is using Cloud storage to give them the ability to access their files (data and information) from any device and any place. Furthermore, Cloud-based data sharing and collaboration provide a very accessible service. For example, a global marketing firm might use cloud storage to enable its employees, spread across different continents, to seamlessly access and collaborate on project files, regardless of their physical location. This feature is crucial for organizations dealing with numerous clients and diverse roles and demands. However, certain security and privacy risks exist within the Cloud environment. The features of multi-tenancy, resource pooling, and shareability, intended to provide benefits, can also be exploited by cybercriminals and individuals with malicious intent, posing threats to both Cloud users and Cloud service providers (Bhajantri & Mujawar, 2019; Krishna et al., 2016; Kumar et al., 2015; Lourens et al., 2022).

In the early 2000s, extensive research focused on cloud data security, highlighting encryption as a key method for protecting data and ensuring privacy. While encryption was effective in making data unreadable and preventing unauthorized access, subsequent studies (Lai et al., 2012; Somani, Lakhani, Mundra, 2010; Xue et al., 2018) indicated that it alone is insufficient in multi-

tenant cloud environments. The imperative for comprehensive security in these shared environments extends beyond encryption, presenting challenges such as potential vulnerabilities in shared resources, internal threats, and the intricate management of encryption keys. These challenges not only heighten the risk of data exposure but also impact the performance of cloud systems. Therefore, a new approach, incorporating robust access control, legal compliance, and a keen focus on performance optimization, becomes essential for ensuring overall data security and system efficiency in the cloud.

To address these challenges, researchers have begun integrating encryption with other solutions such as access control and privacy-preserving schemes (Singh & Singh, 2018) to further enhance data privacy. One scheme that has received considerable attention in research is Attribute-based Encryption (ABE). ABE is a promising solution, offering fine-grained access control and providing data confidentiality on Cloud storage (Sabitha & Rajasree, 2017). Sahai and Waters (Sahai & Waters, 2005) are pioneers of Attribute-based Encryption (ABE) where they claimed that the fine-grained access control scheme is able to support better security services to Cloud users and Cloud Services Providers (CSP). In the present day, numerous investigations have been conducted to enhance ABE, and one form of ABE scheme that has been introduced for this purpose is modified Ciphertext Policy Attribute-based Encryption (CP-ABE).

This chapter briefly overviews the research's context and highlights CP-ABE issues and motives. Then, this chapter provides the primary research objectives and the research's scope. This chapter finishes with a summary of the organisation of the thesis.

1.1 Research Problem

The evolving cloud computing landscape serves as an important platform for comprehensive resource sharing, spanning infrastructure, software, applications and business processes. Achieving the delicate balance between delivering exceptional performance and upholding robust data security poses significant challenges. Cloud Service Providers (CSPs) are expected to provide an efficient platform to ensure uninterrupted system accessibility and availability in addition to protecting data from malicious activities. To meet these expectations, researchers advocate Ciphertext-Based Attribute-Based Encryption (CP-ABE) as a promising solution, providing detailed access control and data confidentiality in cloud storage. CP-ABE, unlike traditional encryption schemes that rely on user identity, allows flexible access control based on attributes associated with the user or data.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE), particularly highlighted by P. Yang et al. (2020), has garnered attention for improving access control and data security. In CP-ABE, each ciphertext is associated with a policy dictating the required attributes for decryption. A user who possesses attributes that

match the policy can decrypt the ciphertext, while those who do not possess the required attributes cannot. This enables fine-grained access control, as the policy can be defined in terms of complex attribute combinations.

In recent years, extensive research has focused on improving CP-ABE, with several studies (Chen, Zhu, Liang, et al., 2021; Hu et al., 2020; Miao et al., 2019; Yang et al. al., 2016; Yang & Jia, 2014) succeeded in prioritizing the achievement of high system security. However, despite these efforts, analysis of this implementation has revealed performance issues making continuous security completely unattainable. Moreover, this extensive research works insufficiently in reducing computational overhead, often neglecting storage costs. This oversight can affect system availability, especially when accessed from low-capacity devices. Addressing these challenges requires a comprehensive approach that not only focuses on improving security but also places a strong emphasis on optimizing CP-ABE system performance. By prioritizing both aspects, efficiency and availability can be achieved. However, there are three outstanding challenges related to privacy and data availability in the Cloud environment with CP-ABE as below:

- Due to its complex structure, the existing CP-ABE scheme struggles to efficiently manage the access policy concealment process. This complexity results in extended processing times, leading to high computation cost. Furthermore, the increased processing duration not only reduces system performance but also compromises privacy protections, leaving user data and privacy more exposed (Jin et al., 2016; Zhang et al., 2019). Consequently, these issues diminish the system's reliability and trustworthiness in protecting sensitive information.

- In CP-ABE, a problem arises when messages contain redundant data. This redundancy exacerbates the inherent issue of increased ciphertext size associated with the number of attributes in the access policy. When messages include repetitive or overlapping data, the resulting ciphertext becomes significantly larger, consuming additional cloud storage space and potentially leading to higher storage costs. This expansion of ciphertext due to data redundancy impacts not only the storage efficiency but also the performance of cloud systems. Larger ciphertexts require more processing power and time for encryption and decryption, slowing down data access and reducing overall system responsiveness (Zhang et al., 2019). These challenges highlight the need for optimizing data management in CP-ABE systems to minimize redundancy, thereby improving storage utilization and maintaining efficient system performance.

- The requirement for frequent and fast decryption of data presents a significant challenge in CP-ABE, especially when numerous tasks require urgent access to encrypted data, causing delays in the scheduling process (Yan et al., 2020). Consequently, during situations where quick data access is crucial, these delays can lead to temporary

data unavailability, impacting decision-making and operational efficiency. This problem underscores the necessity of optimizing the decryption process in CP-ABE systems to ensure timely data access without compromising security.

1.2 Research Questions

The following research questions were considered during the investigation for this study:

- What technique can be used to improve the performance of access policy hiding and providing the privacy in CP-ABE?
- How can an efficiency of CP-ABE be improved in reducing the data storage?
- What is the suitable method to optimize the decryption process?

1.3 Research Objectives

The primary objective of this research is to optimize access policy performance in cloud computing by utilizing a modified Ciphertext Policy Attribute-based Encryption (CP-ABE) approach. This aims to minimize computational overhead, ensure the availability of data, and guarantee data privacy. To achieve this, the following objectives are considered:

- To propose an access policy hiding (APH) scheme utilizing logical connective operations, aimed at reducing the processing time while providing privacy protection.
- To propose a Tokenization Identifier Technique that minimizes the size of message by eliminating the redundancy before they undergo encryption in CP-ABE.
- To propose a task scheduling algorithm based on a priority technique in the decryption phase to decrease response times, thus reducing the unavailability of the required data.

Table 1.1: Comprise the Research Problems (RP), Research Questions (RQ), Research Objectives (RO) and Research Contribution (RC)

RP	RQ	RO	RC
The current CP-ABE scheme struggles to efficiently manage the access policy hiding process due to its complexity, resulting in prolonged processing times and adversely affecting the privacy protection of both data and users.	What technique can be used to improve the performance of access policy hiding and providing the privacy in CP-ABE?	To propose an access policy hiding (APH) scheme utilizing logical connective operations, aimed at reducing the processing time while providing privacy protection.	Access policy Hiding scheme
In CP-ABE systems, the ciphertext size increases with the number of attributes defined in the access policy. Additionally, data redundancy in a message further enlarges the ciphertext, leading to significant inefficiencies in the use of cloud storage.	How can an efficiency of CP-ABE be improved in reducing the data storage?	To propose a Tokenization Identifier Technique that minimizes the size of message by eliminating the redundancy before they undergo encryption in CP-ABE	Tokenization Identifier Technique
The frequent need for fast decryption in CP-ABE, especially with numerous urgent tasks, causes scheduling delays and temporary data unavailability, highlighting the need to optimize the decryption process for timely and secure data access.	What is the suitable method to optimize the decryption process?	To propose a task scheduling algorithm based on a priority technique in the decryption phase to decrease response times, thus reducing the unavailability of the required data.	Priority Task Scheduling algorithm

1.4 Research Scope

The scope of this research is aimed at enhancing the performance and efficiency of Modified Ciphertext Policy Attribute-Based Encryption (CP-ABE). Specifically, it focuses on:

- Optimizing Access Policy Hiding
  - Addressing the challenge of managing access policies in cloud environments where existing schemes lack efficiency, leading to potential privacy breaches.
  - Developing an access policy hiding mechanism that utilizes logical connective operations to optimize APH performance while also providing enhanced privacy protection.

- Reducing data redundancy that led large size encrypted message.
  - Providing an approach in tackling the presence of data redundancy in a message and the direct correlation between the number of attributes in an access policy and the size of the resulting ciphertext, which is exacerbated by the implementation of constant public parameters.
  - Proposing a message size reduction method through a Tokenization Identifier Technique to optimize the size of messages before encryption, aiming to eliminate data redundancy and reduce storage costs.

- Improving data request handling in decryption process.
  - Addressing issues related to large user request with urgency, which lead to response delay during peak times.
  - Developing a task scheduling algorithm that prioritizes decryption requests based on urgency and importance. This approach aims to decrease response times, reduce data unavailability, and enhance overall system responsiveness.

By addressing these focal areas, the research aims to propose a modified CP-ABE approach that minimizes computational overhead, ensures data availability, and guarantees data privacy, thereby making CP-ABE a more viable and effective tool for encryption in cloud storage.

1.5 Thesis Organisation

The subsequent thesis chapters are structured as follows:

Chapter 2 provides an overview of the CP-ABE scheme, including relevant definitions, basics, and principles. Additionally, it identifies various issues and limitations found in the related literature.

Chapter 3 offers a concise presentation of the methodology, mathematical backgrounds, fundamental principles, and key concepts of advanced cryptographic techniques. It also includes a simulation of the benchmark work.

Chapter 4 introduces an access policy hiding mechanism that leverages logical connective operations, designed to minimize encryption times while enhancing privacy safeguards. Additionally, this chapter also presents a pre-processing message reduction strategy employing a Tokenization Identifier Technique, specifically tailored to streamline the size of messages prior to encryption within CP-ABE systems. Furthermore, this chapter proposes a task scheduling algorithm, utilizing a priority-based approach during the decryption phase, aimed at significantly diminishing both waiting and decryption durations. This, in turn, mitigates the issue of data unavailability, ensuring more efficient access to encrypted information.

Chapter 5 discuss Results and Discussion. In this chapter, the proposed APH, TId, PriTask have been tested and verified with discussion through synthetic benchmark datasets and have been compared with an existing technique.

Chapter 6 provides a summary of all the preceding chapters and presents the thesis conclusion. Additionally, it suggests potential directions for future research based on the findings derived from this work.

Summary of thesis structure illustrated in Figure 1.2.

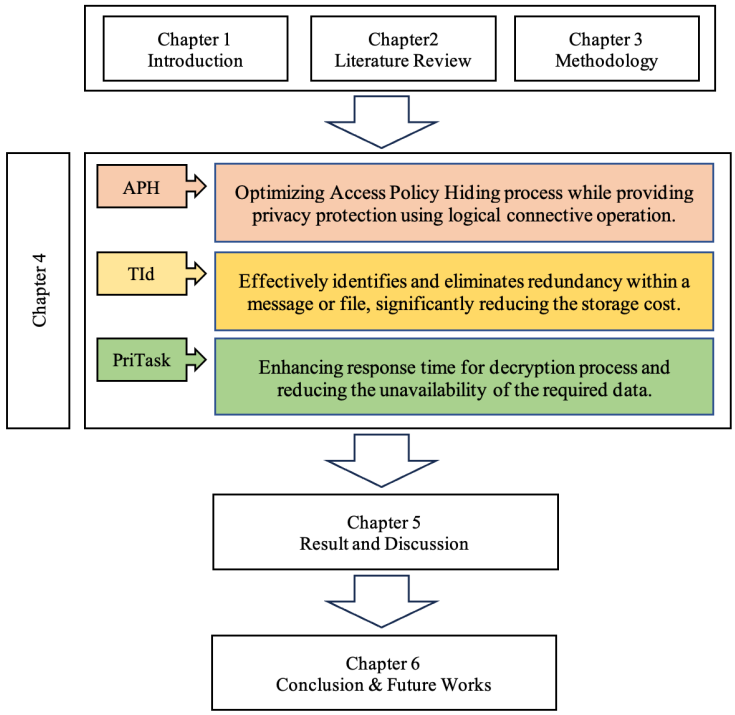

Figure 1.2: The Structure of the Thesis

REFERENCES

Abied, O., Ibrahim, O., & Mat Kamal, S. N.-I. (2022). Adoption of Cloud Computing in E-Government: A Systematic Literature Review. Pertanika Journal of Science and Technology, 30(1), 655–689. https://doi.org/10.47836/pjst.30.1.36

Acheampong, E. M., Zhou, S., Liao, Y., Antwi-Boasiako, E., & Obiri, I. A. (2022). Smart Health Records Sharing Scheme based on Partially Policy-Hidden CP-ABE with Leakage Resilience. 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), 1408–1415. https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00218

Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. Info, 17(1), 54–67. https://doi.org/10.1108/info-09-2014-0042

Aleisa, M. A., Abuhussein, A., & Sheldon, F. T. (2020). Access Control in Fog Computing: Challenges and Research Agenda. IEEE Access, 8, 83986–83999. https://doi.org/10.1109/ACCESS.2020.2992460

Arul Thileeban, S. (2017). Encryption of images using XOR Cipher. 2016 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2016, 4–6. https://doi.org/10.1109/ICCIC.2016.7919607

Banks, J. (2010). Discrete-Event System Simulation. Prentice Hall.

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. https://doi.org/10.1016/j.comnet.2018.01.036

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. 2007 IEEE Symposium on Security and Privacy (SP '07), 321–334. https://doi.org/10.1109/SP.2007.11

Bethencourt, J., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. IEEE Computer Society.

Bhajantri, L. B., & Mujawar, T. (2019). 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, 376–380. https://doi.org/10.1109/I-SMAC47947.2019.9032545

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24–41. https://doi.org/10.1016/j.future.2015.09.031

Chen, E., Zhu, Y., Liang, K., & Yin, H. (2021). Secure Remote Cloud File Sharing with Attribute-based Access Control and Performance Optimization. IEEE Transactions on Cloud Computing, 1–1. https://doi.org/10.1109/tcc.2021.3104323

Chen, E., Zhu, Y., Zhu, G., Liang, K., & Feng, R. (2021). How to implement secure cloud file sharing using optimized attribute-based access control with small policy matrix and minimized cumulative errors. Computers and Security, 107. https://doi.org/10.1016/j.cose.2021.102318

Chen, N., Li, J., Zhang, Y., & Guo, Y. (2022). Efficient CP-ABE Scheme with Shared Decryption in Cloud Storage. IEEE Transactions on Computers, 71(1), 175–184. https://doi.org/10.1109/TC.2020.3043950

Cheng, Y., Ren, J., Wang, Z., Mei, S., & Zhou, J. (2012). Re-encryption optimization in CP-ABE based cryptographic cloud storage. Proceedings - 2nd International Conference on Cloud and Green Computing and 2nd International Conference on Social Computing and Its Applications, CGC/SCA 2012, 173–179. https://doi.org/10.1109/CGC.2012.12

Chinnasamy, P., Deepalakshmi, P., Dutta, A. K., You, J., & Joshi, G. P. (2022). Ciphertext-policy attribute-based encryption for cloud storage: Toward data privacy and authentication in ai-enabled iot system. Mathematics, 10(1). https://doi.org/10.3390/math10010068

Denisow, I., Zickau, S., Beierle, F., & Kupper, A. (2015). Dynamic Location Information in Attribute-Based Encryption Schemes. 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 240–247. https://doi.org/10.1109/NGMAST.2015.63

Domingo-Ferrer, J., Farràs, O., Ribes-González, J., & Sánchez, D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. In Computer Communications (Vols. 140–141, pp. 38–60). Elsevier B.V. https://doi.org/10.1016/j.comcom.2019.04.011

Edemacu, K., Jang, B., & Kim, J. W. (2020). Collaborative Ehealth Privacy and Security: An Access Control With Attribute Revocation Based on OBDD Access Structure. IEEE Journal of Biomedical and Health Informatics, 24(10), 2960–2972. https://doi.org/10.1109/JBHI.2020.2973713

el Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2020). A survey on access control mechanisms for cloud computing. Transactions on Emerging Telecommunications Technologies, 31(2). https://doi.org/10.1002/ett.3720

Emmanuel, B., Dina, H., Cigdem, S., & Vincent, F. (2019). Access Control in the Internet of Things: A Survey of Existing Approaches and Open Research

Questions. Annals of Telecommunications, 74, 375–388. https://doi.org/10.1145/3243734.3243817

Florence, S. M., Alban, S., & Mogalipuvvu, H. (2024). A Hybrid Cryptographic Algorithm for Resource-Constrained IoT Devices. 1914–1918. https://doi.org/10.1109/ic2pct60090.2024.10486560

Fugkeaw, S., & Sato, H. (2016). Key update as a service (KAAS): An agent-based modeling for cloud-based access control. Proceedings - 2016 IEEE International Congress on Big Data, BigData Congress 2016, 430–437. https://doi.org/10.1109/BigDataCongress.2016.67

Gao, S., Piao, G., Zhu, J., Ma, X., & Ma, J. (2020). TrustAccess: A Trustworthy Secure Ciphertext-Policy and Attribute Hiding Access Control Scheme Based on Blockchain. IEEE Transactions on Vehicular Technology, 69(6), 5784–5798. https://doi.org/10.1109/TVT.2020.2967099

Ghaffari, F., Gharaee, H., & Forouzandehdoust, M. R. (2017). Security considerations and requirements for Cloud computing. 2016 8th International Symposium on Telecommunications, IST 2016, 105–110. https://doi.org/10.1109/ISTEL.2016.7881792

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

Han, D., Pan, N., & Li, K. C. (2022). A Traceable and Revocable Ciphertext-Policy Attribute-based Encryption Scheme Based on Privacy Protection. IEEE Transactions on Dependable and Secure Computing, 19(1), 316–327. https://doi.org/10.1109/TDSC.2020.2977646

Hao, J., Huang, C., Ni, J., Rong, H., Xian, M., & Shen, X. (Sherman). (2019). Fine-grained data access control with attribute-hiding policy for cloud-based IoT. Computer Networks, 153, 1–10. https://doi.org/10.1016/j.comnet.2019.02.008

Hu, G., Zhang, L., Mu, Y., & Gao, X. (2020). An Expressive "Test-Decrypt-Verify" Attribute-Based Encryption Scheme With Hidden Policy for Smart Medical Cloud. IEEE Systems Journal, 1–12. https://doi.org/10.1109/jsyst.2020.2996216

Huang, S., Jiang, H., Peng, X., Li, W., & Yu, S. (2021). Secure XOR-CIM Engine: Compute-In-Memory SRAM Architecture With Embedded XOR Encryption. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 29(12), 2027–2039. https://doi.org/10.1109/TVLSI.2021.3120296

Huang, W.-B., Su, W.-T., & Liang, C.-S. (2015). A threshold-based key generation approach for ciphertext-policy attribute-based encryption. 2015 Seventh International Conference on Ubiquitous and Future Networks, 908–913. https://doi.org/10.1109/ICUFN.2015.7182677

Hwang, Y.-W., & Lee, I.-Y. (2019). A Study on Lightweight Anonymous CP-ABE Access Control for Secure Data Protection in Cloud Environment. Proceedings of the 2019 International Conference on Information Technology and Computer Communications, 107–111. https://doi.org/10.1145/3355402.3355405

Jadeja, Y., & Modi, K. (2012). Cloud computing - Concepts, architecture and challenges. 2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012, 877–880. https://doi.org/10.1109/ICCEET.2012.6203873

Jiang, Y., Susilo, W., Mu, Y., & Guo, F. (2016). Ciphertext-policy attribute based encryption supporting access policy update. In L. Chen & J. Han (Eds.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10005 LNCS (pp. 39–60). Springer International Publishing. https://doi.org/10.1007/978-3-319-47422-9_3

Jin, C., Feng, X., & Shen, Q. (2016). Fully secure hidden ciphertext policy attribute-based encryption with short ciphertext size. ACM International Conference Proceeding Series, 88–95. https://doi.org/10.1145/3017971.3017981

Jin, Y., Tian, C., He, H., & Wang, F. (2015). A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing. Proceedings - 2015 IEEE 5th International Conference on Big Data and Cloud Computing, BDCloud 2015, 172–179. https://doi.org/10.1109/BDCloud.2015.57

Junwei, W. (2012). Java realization for Ciphertext- Policy Attribute-Based Encryption. https://github.com/junwei-wang/cpabe/

Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. In Computer Communications (Vol. 111, pp. 120–141). Elsevier B.V. https://doi.org/10.1016/j.comcom.2017.07.006

Kahani, N., Elgazzar, K., & Cordy, J. R. (2016). Authentication and Access Control in e-Health Systems in the Cloud. 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 13–23. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.43

Khan, A. R. (2012). Access control in cloud computing environment. ARPN Journal of Engineering and Applied Sciences, 7(5), 613–615.

Khan, F., Li, H., Zhang, L., & Shen, J. (2017). An Expressive Hidden Access Policy CP-ABE. 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), 178–186. https://doi.org/10.1109/DSC.2017.29

Krishna, B. H., Kiran, S., Murali, G., & Reddy, R. P. K. (2016). Security Issues in Service Model of Cloud Computing Environment. Procedia Computer Science, 87, 246–251. https://doi.org/https://doi.org/10.1016/j.procs.2016.05.156

Kumar, N. S., Lakshmi, G. V. R., & Balamurugan, B. (2015). Enhanced Attribute Based Encryption for Cloud Computing. Procedia Computer Science, 46, 689–696. https://doi.org/https://doi.org/10.1016/j.procs.2015.02.127

Kumar, P., & Alphonse, P. J. A. (2018). Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. *Journal of Network and Computer Applications*, *108*, 37-52.

Kumar, P. V., & Aluvalu, J. A. R. (2015). Key Policy Attribute Based Encryption (KP-ABE): A Review. International Journal of Innovative and Emerging Research in Engineering, 2(2), 49–52.

Lai, J., Deng, R. H., & Li, Y. (2012). Expressive CP-ABE with partially hidden access structures. ASIACCS 2012 - 7th ACM Symposium on Information, Computer and Communications Security, 123, 18–19. https://doi.org/10.1145/2414456.2414465

Lakrami, F., Elkamoun, N., & Kamili, M. El. (2016). Toward a New Extension of the Access Control Model ABAC for Cloud Computing. Lecture Notes in Electrical Engineering, 366, 287–300. https://doi.org/10.1007/978-981-287-990-5

Langaliya, C., & Aluvalu, R. (2015). Enhancing Cloud Security through Access Control Models: A Survey. International Journal of Computer Applications, 112(7), 8–12. https://doi.org/10.5120/19677-1400

Law, A. M. (2003). How To Conduct a Successful Simulation Study. 2003 Winter Simulation Conference, 66–70.

Li, C., He, J., Lei, C., Guo, C., & Zhou, K. (2019). Achieving privacy-preserving CP-ABE access control with multi-cloud. 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications, 801–808. https://doi.org/10.1109/BDCloud.2018.00120

Li, C., Zhang, Y., & Xie, E. Y. (2019). When an attacker meets a cipher-image in 2018: A year in review. Journal of Information Security and Applications, 48. https://doi.org/10.1016/j.jisa.2019.102361

Li, F., Liu, K., Zhang, L., Huang, S., & Wu, Q. (2022). EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem. IEEE Transactions on Services Computing, 15(5), 2755–2765. https://doi.org/10.1109/TSC.2021.3078119

Li, H., Li, J., Zhang, Y., Chen, X., You, I., & Wong, D. S. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences, 379, 42–61. https://doi.org/10.1016/j.ins.2016.04.015

Li, J., Shi, Y., & Zhang, Y. (2017). Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage. International Journal of Communication Systems, 30(1). https://doi.org/10.1002/dac.2942

Li, J. (2016). Research on data access security control mechanism under cloud environment. Proceedings - 2015 International Conference on Intelligent Transportation, Big Data and Smart City, ICITBS 2015, 633–636. https://doi.org/10.1109/ICITBS.2015.161

Li, L., Gu, T., Chang, L., Xu, Z., Liu, Y., & Qian, J. (2017). A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram. IEEE Access, 5(January), 1137–1145. https://doi.org/10.1109/ACCESS.2017.2651904

Li, Y., Zhu, J., Wang, X., Chai, Y., & Shao, S. (2013). Optimized ciphertext-policy attribute-based encryption with efficient revocation. International Journal of Security and Its Applications, 7(6), 385–394. https://doi.org/10.14257/ijsia.2013.7.6.38

Liu, C. W., Hsien, W. F., Yang, C. C., & Hwang, M. S. (2016). A survey of attribute-based access control with user revocation in cloud data storage. International Journal of Network Security, 18(5), 900–916.

Liu, X., Wang, H., Zhang, B., & Zhang, B. (2022). An efficient fine-grained data access control system with a bounded service number. Information Sciences, 584, 536–563. https://doi.org/10.1016/j.ins.2021.10.038

Liu, X., Xia, Y., Yang, W., & Yang, F. (2018). Secure and efficient querying over personal health records in cloud computing. Neurocomputing, 274, 99–105. https://doi.org/10.1016/j.neucom.2016.06.100

Liu, Z., Xu, J., Liu, Y., & Wang, B. (2019a). Updatable Ciphertext-Policy Attribute-Based Encryption Scheme with Traceability and Revocability. IEEE Access, 7, 66832–66844. https://doi.org/10.1109/ACCESS.2019.2918434

Liu, Z., Xu, J., Liu, Y., & Wang, B. (2019b). Updatable Ciphertext-Policy Attribute-Based Encryption Scheme with Traceability and Revocability. IEEE Access, 7, 66832–66844. https://doi.org/10.1109/ACCESS.2019.2918434

Lourens, M., Kaushik, M., Goyal, J., Singh, R., Kuchhal, S., & Tiwari, M. (2022). The Role of Implementing Cloud Computing Technology for Addressing Critical Security Issues and Overcoming the Challenges Effectively. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2303–2306. https://doi.org/10.1109/ICACITE53722.2022.9823892

Lynn, B. (2007). On The Implementation of Pairing-Based Cryptosystems (Issue June).

Mahboob, T., Zahid, M., & Ahmad, G. (2016). Adopting information security techniques for cloud computing - A survey. Proceedings - 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2016, 7–11. https://doi.org/10.1109/ICITISEE.2016.7803038

Malik, A. K., Emmanuel, N., Zafar, S., Khattak, H. A., Raza, B., Khan, S., Al-Bayatti, A. H., Alassafi, M. O., Alfakeeh, A. S., & Alqarni, M. A. (2020). From conventional to state-of-the-art iot access control models. Electronics (Switzerland), 9(10), 1–34. https://doi.org/10.3390/electronics9101693

Malluhi, Q. M., Shikfa, A., & Trinh, V. C. (2017). A ciphertext-policy attribute-based encryption scheme with optimized ciphertext size and fast decryption. ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, 230–240. https://doi.org/10.1145/3052973.3052987

Mansouri, N., & Javidi, M. M. (2017). A Survey of Dynamic Replication Strategies for Improving Response Time in Data Grid Environment. AUT Journal of Modeling and Simulation AUT J. Model. Simul, 49(2), 239–263. https://doi.org/10.22060/miscj.2016.874

Mell, P., & Grance, T. (2011). The NIST-National Institute of Standars and Technology- Definition of Cloud Computing. NIST Special Publication 800-145, 7.

Miao, Y., Liu, X., Choo, K. K. R., Deng, R. H., Li, J., Li, H., & Ma, J. (2019). Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting. IEEE Transactions on Dependable and Secure Computing, 1–15. https://doi.org/10.1109/TDSC.2019.2897675

Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. International Journal of Web Information Systems. https://doi.org/10.1108/IJWIS-04-2022-0077

Nanos, I., Manthou, V., & Androutsou, E. (2019). Cloud Computing Adoption Decision in E-government. Springer Proceedings in Business and Economics, 125–145. https://doi.org/10.1007/978-3-319-95666-4_9

Ning, J., Cao, Z., Dong, X., & Wei, L. (2016). Traceable and revocable CP-ABE with shorter ciphertexts. Science China Information Sciences, 59(11), 5–7. https://doi.org/10.1007/s11432-016-0062-7

Nishide, T., Yoneyama, K., & Ohta, K. (2008). Attribute-Based encryption with partially hidden encryptor-specified access structures.pdf. 111–129.

Niu, X. (2017). Fine-grained access control scheme based on cloud storage. Proceedings - 2017 International Conference on Computer Network,

Electronic and Automation, ICCNEA 2017, 2017-January, 512–515. https://doi.org/10.1109/ICCNEA.2017.48

Nxumalo, Z. C., Tarwireyi, P., & Adigun, M. O. (2015). Towards privacy with tokenization as a service. IEEE International Conference on Adaptive Science and Technology, ICAST, 2015-January. https://doi.org/10.1109/ICASTECH.2014.7068067

Paul, S., Singh, A. P., & Ahmad, S. (2016). Tokenization based service model for cloud computing environment. Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016, 2016. https://doi.org/10.1109/INVENTIVE.2016.7830085

Patil, P. (2022). Healthcare Dataset. In Kaggle. Retrieved from https://www.kaggle.com/datasets/prasad22/healthcare-dataset

Phuong, T. V. X., Yang, G., & Susilo, W. (2016). Hidden ciphertext policy attribute-based encryption under standard assumptions. IEEE Transactions on Information Forensics and Security, 11(1), 35–45. https://doi.org/10.1109/TIFS.2015.2475723

Punithasurya, K., & Priya, J. S. (2012). Analysis of Different Access Control Mechanism in Cloud. International Journal of Applied Information Systems (IJAIS), 4(2), 34–39. www.ijais.org

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science, 110(2012), 465–472. https://doi.org/10.1016/j.procs.2017.06.124

Rashid, A., & Chaturvedi, A. (2019). Cloud Computing Characteristics and Services A Brief Review. International Journal of Computer Sciences and Engineering, 7(2), 421–426. https://doi.org/10.26438/ijcse/v7i2.421426

Revathy, G., Muruga Priya, P., Saranya, R., & Ramchandran, C. (2022). Cloud Storage and Authenticated Access For Intelligent Medical System. Proceedings - 6th International Conference on Computing Methodologies and Communication, ICCMC 2022, 53–56. https://doi.org/10.1109/ICCMC53470.2022.9753765

Rouselakis, Y., & Waters, B. (2015). 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), 8975, 315–332. https://doi.org/10.1007/978-3-662-47854-7_19

Sabitha, S., & Rajasree, M. S. (2017). Access control based privacy preserving secure data sharing with hidden access policies in cloud. Journal of Systems Architecture, 75, 50–58. https://doi.org/10.1016/j.sysarc.2017.03.002

Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In R. Cramer (Ed.), Lecture Notes in Computer Science (pp. 457–473). Springer Berlin Heidelberg. https://doi.org/10.1007/978-1-4419-5906-5_148

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & E.Youman, C. (1996). Role Based Access Control Models. Computer, 29(2), 38–47. https://doi.org/10.1016/S1363-4127(01)00204-7

Sansanwal, S., & Jain, N. (2021). Security Attacks in Cloud Computing: A Systematic Review. Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021, 501–508. https://doi.org/10.1109/ICIRCA51532.2021.9544840

Senthilkumar, S., Brindha, K., Angulakshmi, M., Deepa, M., Gour, M., & Narwani, P. (2020). IMGCRYPTO-XOR Algorithm using MUSIC Theory for secure medical data storage in cloud. 2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE), 1–5. https://doi.org/10.1109/ic-ETITE47903.2020.250

Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4). https://doi.org/10.1002/ett.4108

Sethi, K., Pradhan, A., & Bera, P. (2020). Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation. Journal of Information Security and Applications, 51, 102435. https://doi.org/10.1016/j.jisa.2019.102435

Shyu, S. J. (2018). XOR-Based Visual Cryptographic Schemes with Monotonously Increasing and Flawless Reconstruction Properties. IEEE Transactions on Circuits and Systems for Video Technology, 28(9), 2397–2401. https://doi.org/10.1109/TCSVT.2017.2707923

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. In Journal of Network and Computer Applications (Vol. 79, pp. 88–115). Academic Press. https://doi.org/10.1016/j.jnca.2016.11.027

Singh, N., & Singh, A. K. (2018). Data Privacy Protection Mechanisms in Cloud. Data Science and Engineering, 3(1), 24–39. https://doi.org/10.1007/s41019-017-0046-0

Somani, u. Lakhani, k. Mundra, M. (2010). Implementing digital signatures with R.S.A algorithm to enhance the data security of cloud in cloud computing. 1St International Conference, 211–216.

Souza, S. M. P. C., & Puttini, R. S. (2016). Client-side Encryption for Privacy-sensitive Applications on the Cloud. Procedia Computer Science, 97, 126–130. https://doi.org/10.1016/j.procs.2016.08.289

Sun, P. J. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. IEEE Access, 7, 147420–147452. https://doi.org/10.1109/ACCESS.2019.2946185

Sun, X. (2018). Critical Security Issues in Cloud Computing: A Survey. Proceedings - 4th IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2018, 4th IEEE International Conference on High Performance and Smart Computing, HPSC 2018 and 3rd IEEE International Conference on Intelligent Data and Securit, 1, 216–221. https://doi.org/10.1109/BDS/HPSC/IDS18.2018.00053

Suresh Kumar, S., Chidambaram, G., Vijayalakshmi, S., & Dhayanandh, A. T. (2022). Attribute Based Encryption in Healthcare Application. International Conference on Automation, Computing and Renewable Systems, ICACRS 2022 - Proceedings. https://doi.org/10.1109/ICACRS55517.2022.10029259

Tweneboah-Koduah, S., Endicott-Popovsky, B., & Tsetse, A. (2014). Barriers to Government Cloud Adoption. International Journal of Managing Information Technology, 6(3), 1–16. https://doi.org/10.5121/ijmit.2014.6301

Umesh Chandra Yadav. (2015). Ciphertext-Policy Attribute-Based Encryption with Hiding Access Structure. 2015 IEEE International Advance Computing Conference (IACC), 6–10.

Vaanchig, N., Chen, W., & Qin, Z. (2016). Ciphertext-Policy Attribute-Based Access Control with Effective User Revocation for Cloud Data Sharing System. 2016 International Conference on Advanced Cloud and Big Data (CBD), 186–193. https://doi.org/10.1109/CBD.2016.041

Velte, A. T., Velte, T. J., & Elsenpeter, R. C. (2010). Cloud computing: a practical approach . McGraw-Hill.

Vijayalakshmi, K., & Jayalakshmi, V. (2021). Shared Access Control Models for Big Data: A Perspective Study and Analysis (pp. 397–410). https://doi.org/10.1007/978-981-15-8443-5_33

Vishwesh, J., & Sundaram, S. M. (2017). CP-ABE Protocol for Iot with Cloud. International Journal of Engineering Research & Technology (IJERT), 5(22), 1–3.

Wang, W., Zhang, G., & Shen, Y. (2018). A CP-ABE Scheme Supporting Attribute Revocation and Policy Hiding in Outsourced Environment. 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), 96–99.

Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6571 LNCS(subaward 641), 53–70. https://doi.org/10.1007/978-3-642-19379-8_4

Worapaluk, K., & Fugkeaw, S. (2023). An Efficiently Revocable Cloud-based Access Control Using Proxy Re-encryption and Blockchain. Proceedings of JCSSE 2023 - 20th International Joint Conference on Computer Science and Software Engineering, 178–183. https://doi.org/10.1109/JCSSE58229.2023.10202130

Xiong, H., Zhao, Y., Peng, L., Zhang, H., & Yeh, K. (2019). Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing. Future Generation Computer Systems, 97, 453–461. https://doi.org/10.1016/j.future.2019.03.008

Xue, K., Chen, W., Li, W., Hong, J., & Hong, P. (2018). Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage. IEEE Transactions on Information Forensics and Security, 13(8), 2062–2074. https://doi.org/10.1109/TIFS.2018.2809679

Xue, L., Yu, Y., Li, Y., Au, M. H., Du, X., & Yang, B. (2018). Efficient attribute-based encryption with attribute revocation for assured data deletion. Information Sciences, 0, 1–11. https://doi.org/10.1016/j.ins.2018.02.015

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77. https://doi.org/10.1016/j.micpro.2020.103201

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

Yan, X., Chen, Y., Zhai, Y., Ba, Y., Li, X., & Jia, H. (2020). An Encryption and Decryption Outsourcing CP-ABE scheme Supporting Efficient Ciphertext Evolution. Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, 116–125. https://doi.org/10.1145/3377644.3377669

Yang, K., Han, Q., Li, H., Zheng, K., Su, Z., Shen, X., Member, S., & Su, Z. (2016). An Efficient and Fine-Grained Big Data Access Control Scheme with Privacy-Preserving Policy. IEEE Internet of Things Journal, 4(c), 1–8. https://doi.org/10.1109/JIOT.2016.2571718

Yang, K., & Jia, X. (2014). Expressive , Efficient , and Revocable Data Access Control for Multi-Authority Cloud Storage. IEEE Transactions on Parallel and Distributed Systems, 25(7), 1735–1744.

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. In IEEE Access (Vol. 8, pp. 131723–131740). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.3009876

Yi, S., Wang, Z., Ma, S., Che, Z., Huang, Y., & Chen, X. (2010). An Effective Algorithm of Jobs Scheduling in Clusters. In Article in Journal of Computational Information Systems (Vol. 6, Issue 10). http://www.Jofcis.com1553-9105/

Yin, H., Li, Y., Li, F., Deng, H., Zhang, W., & Li, K. (2022). An efficient and access policy-hiding keyword search and data sharing scheme in cloud-assisted IoT. Journal of Systems Architecture, 128. https://doi.org/10.1016/j.sysarc.2022.102533

Ying, Z., Wei, L., Li, Q., Liu, X., & Cui, J. (2018). A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud. IEEE Access, 6, 53698–53708. https://doi.org/10.1109/ACCESS.2018.2871170

Younis, Y. A., Kifayat, K., & Merabti, M. (2014). An access control model for cloud computing. Journal of Information Security and Applications, 19(1), 45–60. https://doi.org/10.1016/j.jisa.2014.04.003

Younis, Y. A., Kifayat, K., & Merabti, M. (2016). A novel evaluation criteria to cloud based access control models. In Proceedings - 2015 11th International Conference on Innovations in Information Technology, IIT 2015 (pp. 68–73). https://doi.org/10.1109/INNOVATIONS.2015.7381517

Zafar, F., Khan, A., Ur, S., Malik, R., Ahmed, M., Anjum, A., Khan, M. I., Javed, N., Alam, M., & Jamil, F. (2017). A survey of cloud computing data integrity schemes : Design challenges , taxonomy and. Computers & Security, 65, 29–49. https://doi.org/10.1016/j.cose.2016.10.006

Zeng, P., Zhang, Z., Lu, R., & Choo, K. K. R. (2021). Efficient Policy-Hiding and Large Universe Attribute-Based Encryption with Public Traceability for Internet of Medical Things. IEEE Internet of Things Journal, 8(13), 10963–10972. https://doi.org/10.1109/JIOT.2021.3051362

Zhang, L., Cui, Y., Mu, Y., & Member, S. (2020). Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. IEEE SYSTEMS JOURNAL, 14(1), 1–11. https://doi.org/10.1109/JSYST.2019.2911391

Zhang, L., Hu, G., Mu, Y., & Rezaeibagha, F. (2019). Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system. IEEE Access, 7, 33202–33213. https://doi.org/10.1109/ACCESS.2019.2902040

Zhang, L., Su, J., & Mu, Y. (2020). Outsourcing Attributed-Based Ranked Searchable Encryption with Revocation for Cloud Storage. IEEE Access, 8, 104344–104356. https://doi.org/10.1109/ACCESS.2020.3000049

Zhang, R., Ma, H., & Lu, Y. (2017). Fine-grained access control system based on fully outsourced attribute-based encryption. Journal of Systems and Software, 125, 344–353. https://doi.org/10.1016/j.jss.2016.12.018

Zhang, Y., Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based Encryption for Cloud Computing Access Control: A Survey. In ACM Computing Surveys (Vol. 53, Issue 4). Association for Computing Machinery. https://doi.org/10.1145/3398036

Zhang, Y., Zheng, D., & Deng, R. H. (2018). Security and Privacy in Smart Health : Efficient Access Control. IEEE Internet of Things Journal, 5(3), 2130–2145. https://doi.org/10.1109/JIOT.2018.2825289

Zhang, Z., Zhang, W., & Qin, Z. (2021). A partially hidden policy CP-ABE scheme against attribute values guessing attacks with online privacy-protective decryption testing in IoT assisted cloud computing. Future Generation Computer Systems, 123, 181–195. https://doi.org/10.1016/j.future.2021.04.022

Zhao, C., Xu, L., Li, J., Fang, H., & Zhang, Y. (2022). Toward Secure and Privacy-Preserving Cloud Data Sharing: Online/Offline Multiauthority CP-ABE With Hidden Policy. IEEE Systems Journal. https://doi.org/10.1109/JSYST.2022.3169601

Zickau, S., Thatmann, D., Butyrtschik, A., Denisow, I., & Axel, K. (2016). Applied Attribute-based Encryption Schemes. 19th International ICIN Conference - Innovations in Clouds, Internet and Networks, March, 1–3.