INTI JOURNAL | Vol.2024:26
eISSN:2600-7320

Secure Cloud Storage with a Sanitizable Access Control System Again Malicious Data Publisher

Alfiya khanum R M [1], Chitra K[1], Noor Zuhaili Md Yasin[2]

[1]Dayananda Sagar Academy of Technology and Management, Karnataka, India
[2]Faculty of Data Science & IT, INTI International University, 71800 Nilai, Negeri Sembilan, Malaysia

Email: alfiyakhanum15@gmail.com, chitra-mca@dsatm.edu.in, noorzuhaili.mdyasin@newinti.edu.my

Abstract

A novel encryption mechanism known as Ciphertext Policy of topic has been developed. Attribute Based Encryption (CPABE) was developed as an alternative to password-based systems to address the challenges associated with secure data sharing, where users are required to know the password for each file they need. This research work proposes a CPABE-based approach where just one secret key is required per user. A strategy has been implemented to establish precise document access control in a typical academic environment. Only users with the specified attribute similar to public key cryptography, can be encrypted many times to satisfy the access structure defined and allowing different users to decode the contents for secret retrieval. CP-ABE only necessitates a single encryption for each document due to its encoding. The idea of CPABE, which stands for Ciphertext-Policy Attribute-Based Encryption and analyses it in relation to other types of ABE, which stands for attribute-based encryption is developed here.

Keywords

Public Key Cryptography, Fine-Grained Access Control, Discusses Conventional Public Key Cryptography, The Ciphertext Policy-attribute based Encryption (CPABE), CPABE-based Solution for Granular fetching control of access policy

1. Introduction

In ciphertext-policy attributed-based encryption (CP-ABE), the encryptor assigns a label, known as an access structure or ciphertext policy, to each ciphertext. Additionally, each private key is linked to a specific set of attributes [S. K. Pasupuleti, 2015]. For a user to decrypt a ciphertext, it is necessary and sufficient that the attributes of his private key meet the access structure defined by the CPABE scheme for different attributes, file formats, and file sizes [C. Wang et al., 2014; D. Boneh et al., 2004]. Multiple essential documents required by numerous personnel must be stored on company servers in modern paperless offices. Each document in this scenario must be accessible only to a specific group of authorized individuals. The policy for encrypting ciphertext is based on permitted access [Soe Myint Myat and Than Naing Soe, 2020], which is a clear requirement. In the case of an ATTRIBUTES instance, every staff from any

Submission: 4 May 2024; **Acceptance:** 6 August 2024

department would have the ability to access any document if the information is available on a single server. Codification is a method of encoding and conveying data in an unintelligible form [D. Zissis and D. Lekkas, 2019]. To utilize typical asymmetric key cryptography or password-based approaches [Soe Myint Myat and Than Naing Soe, 2020], each user must possess a corresponding number of passwords or public/secret key pairs equivalent to the number of files they intend to access. Waters' initial introduction of Attribute-Based Encryption (ABE) [Soe Myint Myat and Than Naing Soe, 2020; Z. Wang et al., 2015] brought about a significant transformation in public key cryptography, enabling the development of a more efficient access control system compared to conventional public key encryption methods. This technique involves encoding a message based on an access control policy and the attribute set linked to the private key used for decryption can only be used if it satisfies the constraints of the access policy. The use of granular access control to provide varying levels of authorization to the group of end-users or individuals. Ciphertext Policy-Attribute Based Encryption (CP-ABE)-based predicated proposition for fine-grained view control of institute papers [M. Mahdavi et al., 2024], where fastidious partaking is necessary for critical instrument hosted on a partake locality for each faculty to post grades.

2. Literature Survey

There is a limited number of Attribute-Based Encryption techniques available that utilize a reliable server for data storage [K. Hasegawa et al., 2016]. There is always a possibility of a "insider attack" on the data by someone who has authorized access to the server, even when user checks are implemented to allow a user to access a specific piece of data.

Fine-Grained Access Control of Encrypted Data shows the use ABE variations to enable fine-grained access control on data. The method does not handle the intricate rules necessary for a variety of applications, such as broadcasting a message at a university for only HOD or upper management to see. CP-ABE systems, where users are characterized by a variety of qualities, are more beneficial for such advanced broadcast encryption. The suggested method encrypts a message using an access tree and decrypts it using Lagrange interpolation.

A functional encryption library implementation (also unknown as ABE in general) was suggested by Keisuke [Keisuke et al, 2016] as a tool for cloud server data access control. By using an organization’s access policy, they demonstrated the tool. A few further ABE uses have been suggested in the literature. To the best of our knowledge, this is the first time it has attempted to be applied in a university setting.

2.1 Attribute based encryption (ABE)

Attribute-based encryption is an asymmetric key decryption method that enables any end user to be identified based on a set of attributes, such as their name, department, and position. In a standard public key cryptography system, there are two keys: a confidential key known only to the recipient of the message, and an asymmetric key known to everyone. When User1 desires to transmit a secure communication to User2, User1 employs User2's public key to encrypt the message. User 2 subsequently decrypts the information utilizing the exclusive key.

Figure 1 illustrates the standard configuration of asymmetric key cryptography [Z. A. Hussien et al., 2023]. Suppose a data owner adheres to the usual protocol and uploads an encrypted file named Filel to the primary data store, together with the corresponding public keys for Users 1, 2, and 3. Subsequently, three separate ciphertext files are generated, namely CT1: 1, CT2: 1, and CT3: 1.Only the secret key belonging to User1 has the ability to decrypt the Ciphertext file CT1, whereas only User2's private key and User3's key PURI can decrypt Ciphertext file CT3. This decryption process requires the involvement of a trustworthy authority. Every user employs the global public key to encrypt a file and utilizes a private key with distinct characteristics to decrypt it. During data encryption, access controls are assigned by applying computational operators to those attributes. A networked availability strategy is established to determine the conditions for entrance. Access requirements are provided for structure tree 12, where the internal nodes are tied to a certain set of characteristics.

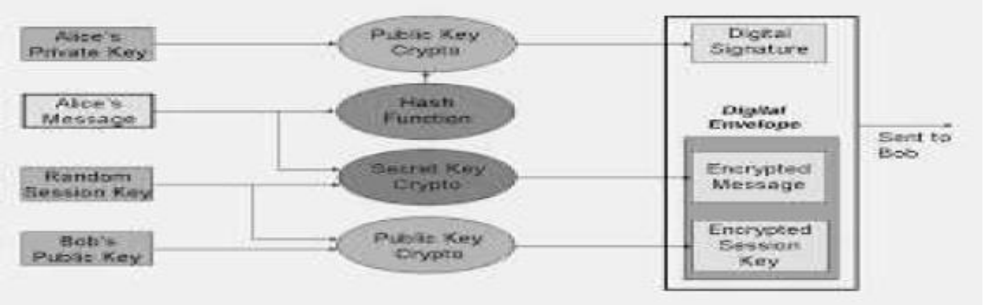


Figure 1: Asymmetric key secret writing system

Suppose a Data administrator wants to preserve Filel for as long as feasible, which is associated with a specified set of attributes then attribute-based encryption technique is required. Suppose a Data administrator wishes to preserve Filel for as long as possible, then a system has n users, traditional public key cryptography will produce n separate ciphertext files and n keys, but attribute-based encryption will only produce a one of the codes of secret message file with n+1 keys. Thus, both the storage of plaintext and the time required for encryption are reduced.

2.2 Authentication according to protocol properties

All users can utilize the global public key in CP-ABE. The customer's confidential key is linked to a distinct set of properties. During data encryption, access controls are allocated using computational operators on those qualities. An availability strategy that is based on network connections is established for determining entrance conditions. The access criteria are defined using a tree structure, where internal nodes represent logical operators and external nodes represent different attributes. Operators and leaf nodes possess distinct characteristics. Only users possessing the specific qualities assigned during the creation of the key can access and view the encrypted data items [Oleksii Zarichuk, 2024]. The ability to get conditions refers to the logical equations that are created while integrating logical processors with information included in a parameter list. The logic gates OR, AND, and threshold gates with t out of n agreement can be employed to establish the access criterion. Matching the conditions for privileges. The while generator consists of n threshold gates, all of which are active. In contrast, the OR constructor just requires one active threshold gate out of n total. Individuals lacking their respective credentials have the ability to decipher a text that has been encoded using a cypher. Record boundaries are defined and incorporated into the file throughout the process of safeguarding. Figure 2 illustrates an example of the system strategy. The data owner utilizes access policy T to encrypt message M. When users' attribute sets meet the requirements of T, user can decrypt the ciphertext.

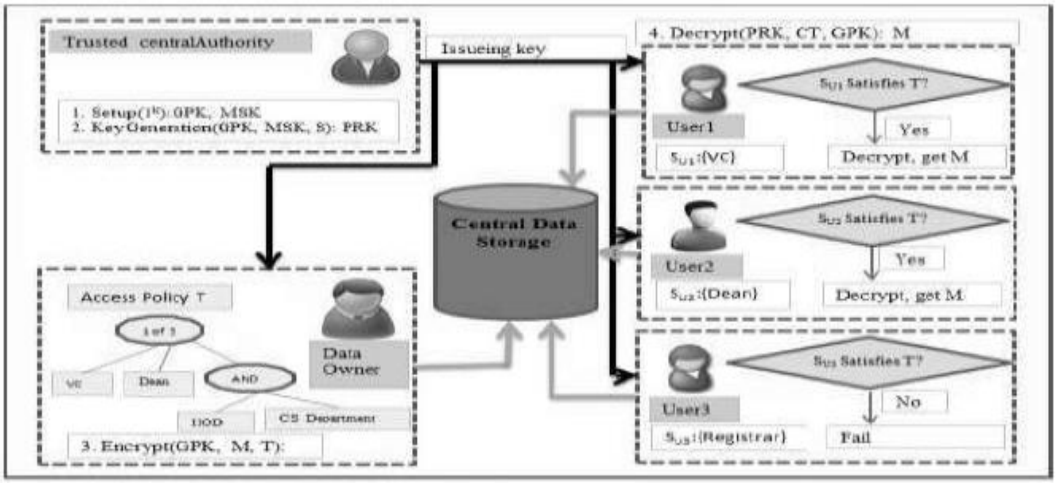


Figure 2: An example of CP-ABE scheme

Development of Proposed CP-ABE

The CP-ABE scheme provides a set P of descriptor qualities that are associated with private keys. The user utilizes an access tree structure, denoted as T, to explicitly define the access policy for encrypting a communication. The inside nodes correspond to threshold gates or logic operators. The threshold value of a node will be equal to the number of its internal children, which are numbered from 1 to N. The threshold gate functions as an OR operator when the value is 1, and as an AND operator when the value is not 1. The property value associated with the node is represented by the external leaf node. The CP-ABE system under consideration is constructed via bilinear pairing e, which involves two multiplicative cyclic groups of prime order p, and is employed for performing pairing operations. The bilinear map satisfies the following two criteria: Bilinearity refers to a property or characteristic of a mathematical function or operation that is linear in each of its two arguments. This requirement asserts that the mapping function must adhere to the equation below.

1. **Bilinearity and Non-Degeneracy**
2. **Lagrange Coefficient**

This method is essential for ensuring that the decryption process can accurately reconstruct the original polynomial used during encryption.

- • Encrypt: This technique uses the provided access policy, also referred to as the tree access structure T, to encrypt a file. A polynomial is assigned to every node x, whether it is an internal or exterior node, in the tree T. The polynomial q is chosen in a hierarchical manner, starting at the root node of the tree T. Each node x in the polynomial q is assigned a degree d, which is equal to the threshold value k 1.

- To initiate the process, this method straightforwardly invokes the DecryptNode function (CT, PRK, root) on the root node of the access tree T. Given that the set of features S fulfils the access policy, we assign R the value obtained from decrypting the node using CT, PRK, and the root. Subsequently, the decryption procedure computes (e(C, D) R). Derived from the CP-ABE implementation.

2.3 Issues and Situation

This research study utilized a university as a case study, where records are stored in a centralized manner at a certain location, such as Locationl. These statistics are accessible to all scholars in any field of study. Figure 3 displays the presumed organizational framework for academic personnel at universities.

University Organization Chart

Figure 3: An organizational structure for academic staff

Content-based encryption, often known as CP-ABE (Ciphertext-Policy Attribute-Based Encryption), is a cryptographic technique. We want to enforce the limitation that only faculty members from Department D1 who hold the positions of Professor, Associate Professor, or Assistant Professor, as well as the Head of Department (HOD) teaching the subject Sujectl (Lecture, Tutorial, or Lab of B5 batch), the theory or lab coordinator for this subject, the In-charge of Subjectl in EVEN semester 2017, the In-charge of 2nd Semester D1 2017, or the In-charge of D1 2017, are allowed to access this file. In addition, all individuals have access to this information until the end of the 2017 EVEN semester. However, starting from that point, the Head of the D1 department, the Dean, and the Vice Chancellor will also have access. Figure 5 illustrates typical role hierarchy of academy employees in university.

Every employee possesses distinct attributes, and the file may be accessed through a local server named Locationl. The file in question is titled Subjectl_D1_B5_Sem2_Lab_Marks_EVEN_2017.doc. The department is identified as D1, the batch is labelled as B5, and the semester is denoted as Sem 2. Access to this confidential marks file should be limited to the faculty members associated with this specific batch. Due to the file being stored on a shared server, it is accessible to anybody. Implementing password security can effectively restrict unauthorized access to files.

However, it is important to note that password-based authentication comes with practical difficulties, as previously mentioned. The file must be stored in an encrypted format to ensure that only authorized individuals with authorization can retrieve it. To implement precise access control for university grades data, we have implemented a Ciphertext Policy-Attribute system [S. AlGhamdi et al., 2020].

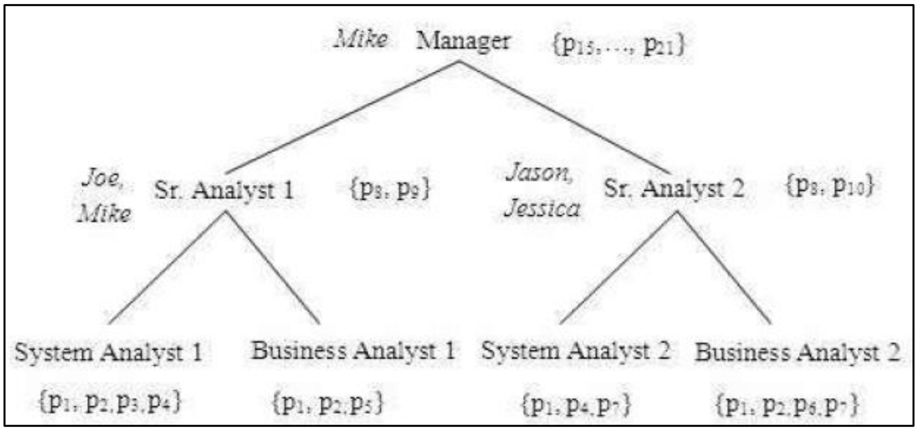
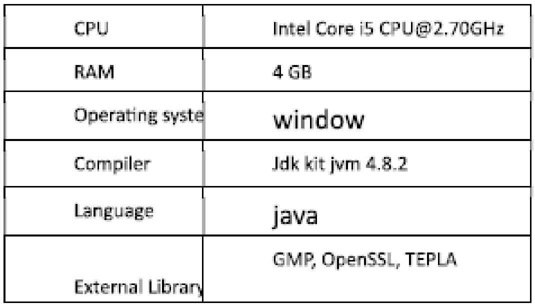


Figure 4: Typical Role hierarchy of Academy Employees in University

Solution based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The setup procedure produces the Global Public Key (GPK) and Master Secret Key (MSK) file. The GPK (Global Public Key) and MSK (Master Secret Key) are utilized to derive the private key for each individual user. The private key of a user is generated by using the values of their attributes as input. To securely store a file on Locationl, it is necessary to apply an access policy to the data using the encryption command. It is important to ensure that only faculty members affiliated with Department D1 who hold the positions of Professor, Associate Professor, or Assistant Professor have access to this file until the end of the EVEN semester 2017. However, after that, the Head of the Department (HOD) of D1, the dean, and the Vice Chancellor (VC) may also examine the file. Figure 5 illustrates the hierarchical structure of the access policy's access tree in this particular situation. Every employee possesses a variety of distinct attributes, and only those workers who satisfy the access criteria can gain access to the file. Table I presents a comprehensive summary of the traits possessed by each employee. The private keys of each user are produced using the attribute values.

To utilize CP-ABE, the user needs to decode the file named Subject1_D1_B5_Sem2_Lab_Marks_EVEN_2017.doc located at Location1. This decryption process requires the user's private key, UPRK, which was issued by a central authority based on the user's specific set of characteristics, S. If the user possesses the necessary attributes that align with the access policy, T, specified in the encrypted file, the file will be decrypted successfully using the user's key.



CPU	Intel Core i5 CPU@2.70GHz
RAM	4 GB
Operating syste	window
Compiler	Jdk kit jvm 4.8.2
Language	java
External Librar	GMP, OpenSSL, TEPLA

Figure 5: Setting description used for the tests

3. Results and Discussions

Some tests were conducted on fake users, their set of characteristics, and various document sizes to evaluate the performance of CP-ABE based encryption and decryption. Regarding a variety of features, this work have examined how well the key generation, encryption, and decryption processes performed [J. Li et al., 2005]. Figures 7 and 8 present the findings decryption time and key generation stage.

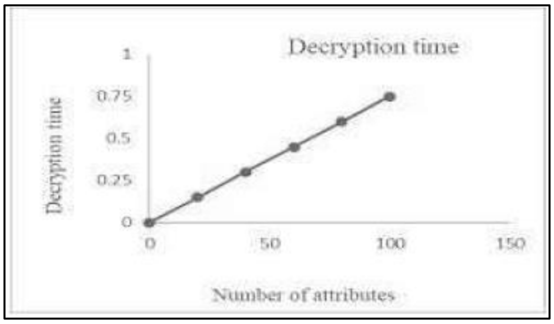


Fig.6.Decription time 1

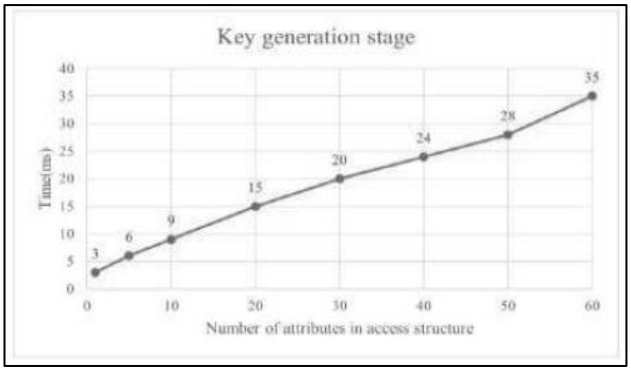


Fig.7. Key generation stage

The figure, labelled as Fig. 7, displays the precise calculation durations for the secret key generation process of our CP-ABE system, considering various amounts of user-specific features. The key generation time remains constant when there are 2 to 4 characteristics. When the number of characteristics is increased from 4 to 6, the time required to generate the key increases significantly in a linear manner. The time required for key creation consistently grows as the number of attributes continues to increase. The utilization of stochastic numbers, specifically Z in exponentiation, is the underlying factor behind the seeming unpredictability in the production time of cryptographic keys, which is observed across several attributes associated with the secret key. The time required for key generation frequently increases in a linear manner with the number of criteria utilized in determining the access policy. During the process of decryption, the linear relationship becomes less apparent. The decryption time is determined on the specific access trees and collection of features employed. Increasing the number of comparisons results in a proportional increase in the time required for decryption. We employed distinct users' individual private keys to decrypt the identical ciphertext, which had been encrypted using the same access policy.

4.Conclusion

To show the practical application of CP-ABE for the purpose of implementing fine-grained access control of documents, a university scenario has been utilized. Access to documents that are stored in a central location is restricted to just those users who satisfy the requirements of the access policy's attribute value. It has been proved to be an efficient cryptographic solution in comparison to traditional public key cryptography. This is because it requires a decreased number of keys and encrypted documents to be generated. There is the possibility of pursuing further expansion of the work to add document partial encryption and decryption through the utilization of CP-ABE.

References

S. K. Pasupuleti, “Privacy-Preserving Public Auditing and Data Dynamics for Secure Cloud Storage Based on Exact Regenerated Code,” International Journal of Cloud Applications and Computing, vol. 9, no. 4, pp. 1–20, Oct. 2019, doi: https://doi.org/10.4018/ijcac.2019100101.

C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, Feb. 2013, doi: https://doi.org/10.1109/tc.2011.245..

D. Boneh, B. Lynn, and H. Shacham, “Short Signatures from the Weil Pairing,” Journal of Cryptology, vol. 17, no. 4, pp. 297–319, Jul. 2004, doi: https://doi.org/10.1007/s00145-004-0314-9.

D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2019, doi: https://doi.org/10.1016/j.future.2010.12.006.

K. Hasegawa, Naoki Kanayama, Takashi Nishide, and E. Okamoto, “Software Library for Ciphertext/Key-Policy Functional Encryption with Simple Usability,” Journal of Information Processing, vol. 24, no. 5, pp. 764–771, Jan. 2016, doi: https://doi.org/10.2197/ipsjjip.24.764.

Soe Myint Myat and Than Naing Soe, “Preserving the Privacy for University Data Using Blockchain and Attribute-based Encryption,” Feb. 2020, doi: https://doi.org/10.1109/icca49400.2020.9022852.

Z. Wang, D. Huang, Y. Zhu, B. Li, and C.-J. Chung, “Efficient Attribute-Based Comparable Data Access Control,” vol. 64, no. 12, pp. 3430–3443, Dec. 2015, doi: https://doi.org/10.1109/tc.2015.2401033.

M. Mahdavi, Mohammad Hesam Tadayon, Mohammad Sayyad Haghighi, and Z. Ahmadian, “IoT-friendly, pre-computed and outsourced attribute-based encryption,” Future Generation Computer Systems, vol. 150, pp. 115–126, Jan. 2024, doi: https://doi.org/10.1016/j.future.2023.08.015.

Z. A. Hussien et al., “Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems,” Applied Sciences, vol. 13, no. 2, p. 691, Jan. 2023, doi: https://doi.org/10.3390/app13020691.

Oleksii Zarichuk, “Security in cloud computing: Methods for ensuring privacy and integration in modern applications,” *Upravlìnnâ rozvitkom*, vol. 23, no. 1, pp. 37–45, Feb. 2024, doi: https://doi.org/10.57111/devt/1.2024.37.

X. Tan, Q. Xie, L. Han, S. Wang, and W. Liu, “Proof of retrievability with flexible designated verification for cloud storage,” *Computers & Security*, vol. 135, pp. 103486–103486, Dec. 2023, doi: https://doi.org/10.1016/j.cose.2023.103486.

P. McDaniel and A. Prakash, “Methods and limitations of security policy reconciliation,” ACM Transactions on Information and System Security, vol. 9, no. 3, pp. 259–291, Aug. 2006, doi: https://doi.org/10.1145/1178618.1178620.

K. Hasegawa, Naoki Kanayama, Takashi Nishide, and E. Okamoto, “Software Library for Ciphertext/Key-Policy Functional Encryption with Simple Usability,” Journal of Information Processing, vol. 24, no. 5, pp. 764–771, Jan. 2016, doi: https://doi.org/10.2197/ipsjjip.24.764.

S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, “Information Security Governance Challenges and Critical Success Factors: Systematic Review,” *Computers & Security*, vol. 99, p. 102030, Sep. 2020, doi: https://doi.org/10.1016/j.cose.2020.102030.

J. Li, N. Li, and W. H. Winsborough, “Automated trust negotiation using cryptographic credentials,” Nov. 2005, doi: https://doi.org/10.1145/1102120.1102129.