ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s

Ciphertext-Policy Attribute-Based Encryption for Cloud Environment with Secured Access Policy

P. Prathap Nayudu

Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Abstract: Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has emerged as a promising cryptographic technique for enhancing data security and access control in cloud environments. This paper presents a comprehensive study on designing and implementing Secured Access Policies within CP-ABE frameworks. We propose a novel approach that combines attribute-based encryption with fine-grained access control, allowing data owners to specify intricate access policies for their encrypted data. Our solution addresses the challenges of scalability, key management, and policy expressiveness in cloud-based scenarios. We provide a detailed analysis of the proposed Secured Access Policy framework, highlighting its advantages and practical implications.

Keywords: Ciphertext-Policy Attribute-Based Encryption, Cloud Security, Access Control, Data Privacy, Key Management, Secured Access Policy, Fine-Grained Access Control, Encryption, Cloud Deployment.

1 Introduction

Cloud computing has been one of the most critical information technology techniques since 2007. The government and industry have paid much attention to this technology [1]. There are four main components to enhance the performance of the cloud that are Service-Oriented Architecture (SOA), virtualization, a variety of services, and deployment architecture [2]. It provides services in the form of payment when you use it. Many features are available, including cost, measurement, and on-demand access to use resources efficiently. The cloud offers many advantages to users, but still, there exist some challenges in security and data storage. Data stored in the cloud is generally sensitive and confidential, such as medical data and military information [3]. To protect data, additional security measures like authentication and access control are necessary. It is critical to encrypt users' data before it is outsourced to the cloud to achieve advanced data protection [4].

An access policy structure is generated based on the user's attribute. To improve the access policy's privacy, the SHA-512 algorithm is presented [5].

- To decrease the loss of data, the CP-ABE algorithm is presented. It is used to encrypt sensitive data. The effectiveness of the proposed approach is analyzed based on different metrics such as security level, encryption time, decryption time, uploading time, downloading time, and memory

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s
usage.

2 Literature Survey

Many researchers have developed access policies based on secure data transactions on the cloud. Some of the works are analyzed here;[6] developed an encryption approach based on ciphertext policies for cloud storage. In this approach, the authors developed a CP-ABE model for user data security and privacy enhancement by hiding the access policy. Then, the authors generated a constant-size ciphertext to reduce the storage overhead. Besides, they used a short signature scheme to identify the inside attackers [7]. Furthermore, they developed a secure fine-grained access control system in this approach. They compared
the model's performance with other CP-ABE methods, and the results showed the outperformance of the model.

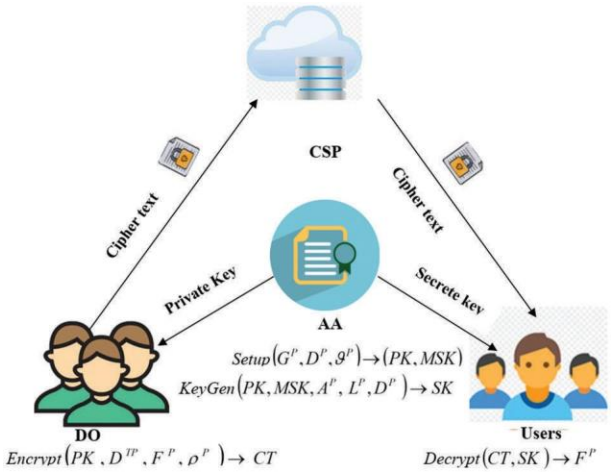


Figure 1: System model

In Fig. 1, CSP is used to store data from DOs. Users can retrieve data from the CSP depending on their requests. However, this is not entirely reliable. They need to have data files for their users. DOs' data files are stored in CSP and may be shared with users via CSP. DOs encrypt data files and may define an access policy [8-10]. Finally, they save the ciphertext (CT) to the CSP. AA is the central hub for the formation of PK and SK. It
assigns PK to DO as well as SK to users. Thus each user can attain different access rights depending on their attributes.

The main objective of the proposed methodology is to securely access the data on the cloud using a secured access policy with CP-ABE [11]. Initially, the data stored in the cloud are encrypted using

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s
CP-ABE.

To enhance the CP-ABE's performance, the access policies are encrypted using the SHA-512 algorithm. It leads to a decrease in the users' information leakage [12]. The proposed system consists of three main stages that are the registration phase, the secure data uploading stage, and the decryption stage. The
structure of the proposed methodology is given in Fig. 2.

2.1 Registration Phase

The registration phase is a significant stage for secure data transactions on the cloud. In this phase, initially, the users register their details in the cloud for data access. Before using the system, they must apply for approval as an administrator [13]. Typically, users will be asked to register their username or username, password, age, and gender.

2.1.1 Login Phase

A login is a set of certificates used to verify a customer. Often, this will contain a username with a password. Logins are used to obtain login and command of any PCs or administrations. The client enters his client ID with the secret key for information access. During the verification phase, the system checks whether the user is authorized or not.

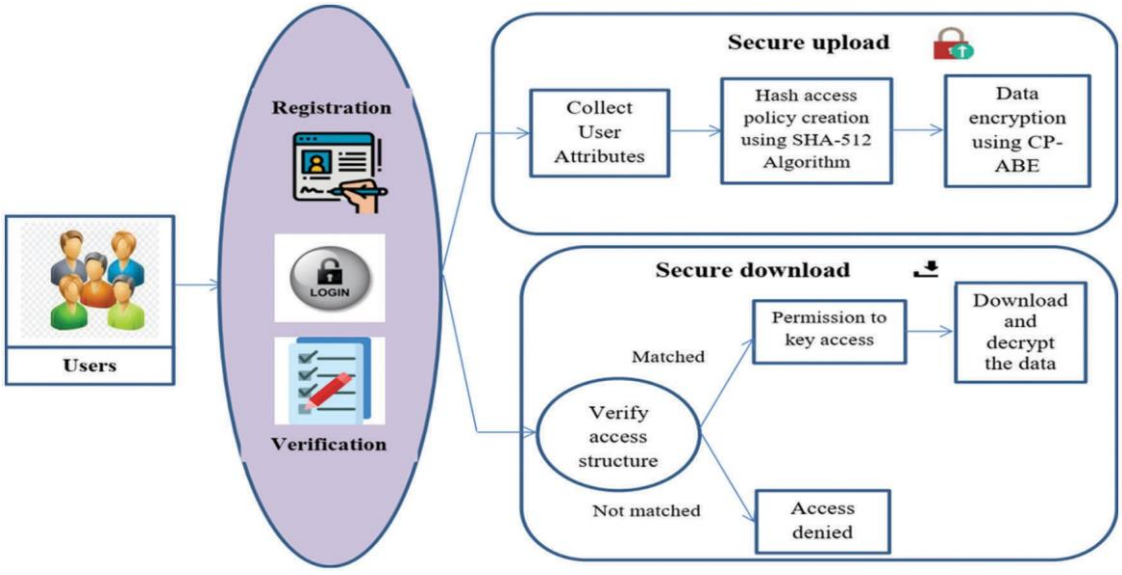


Figure 2: Structure of proposed secure data transmission

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s

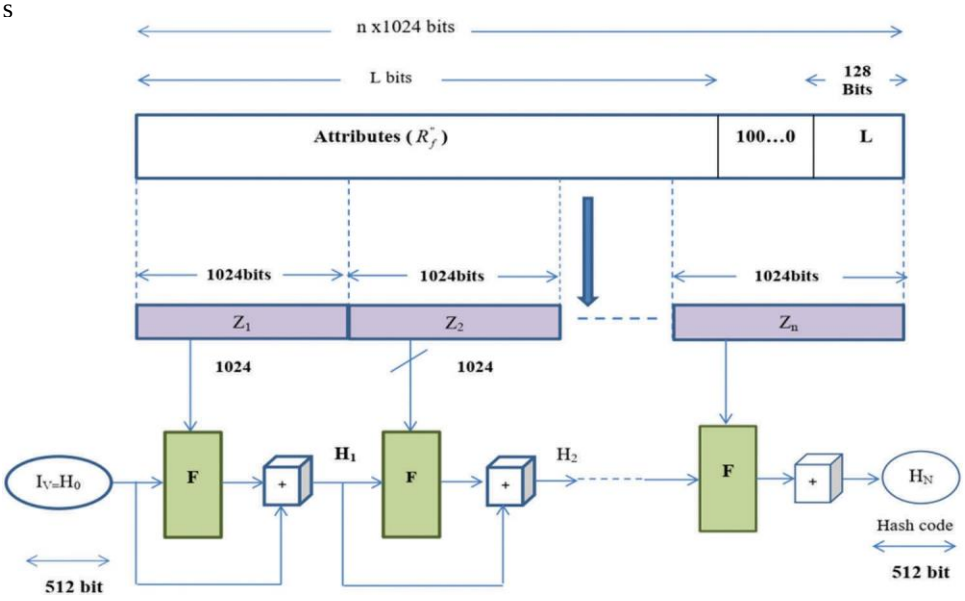


Figure 3: Structure of the proposed SHA-512 algorithm

The technique consists of four stages: input design, hash cache initialization, message processing, and output. Each stage explanation is given below;

- Input formatting

Consider the input message and check that the message size is suitable for further processing. If the size of the input message is sufficient, any padding bits will not be added to it; otherwise, padding bits will be used to get the required size. Typically, the padding bits are '1' and multiple '0's (100000 … 000). Also,
according to SHA-512, there should be even a bit of padding. So a single dump bit would simply be '1'.
Here, it connects the 128-bit module with the input message. Also, this module contains the unsigned
128-bit integer (originally the most significant byte) and the length of the original input message (before dumping). The end of those two steps will reach a message with a length of 1024 bits. The expanded message is signified as the Results and Discussion

The experimental results of the proposed approach are analyzed in this section. This proposed scheme is implemented using Java with the Windows 7 operating system on a 2 GHz dual-core PC machine with 4 GB of main memory. The performance of the proposed HCP-ABE is analyzed based on encryption time, decryption time, key build time, security level, memory usage in encryption, and memory usage in decryption. Besides, the performance of the proposed HCP-ABE is compared with that of the conventional CP-ABE and ABE schemes.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s

Security is one of the most critical parameters in the cloud because the cloud is an unreliable network. For security purposes, in this paper, the HCP-ABE algorithm is utilized. Fig. 4 shows the security level ofdifferent methods. When analyzing Fig. 4, the proposed method attained a high-security level compared to the other two methods, namely CP-ABE-based security and ABE-based security. Also, from the figure, ABE- based security attained the worst security level compared to CP-ABE and HCP-ABE.

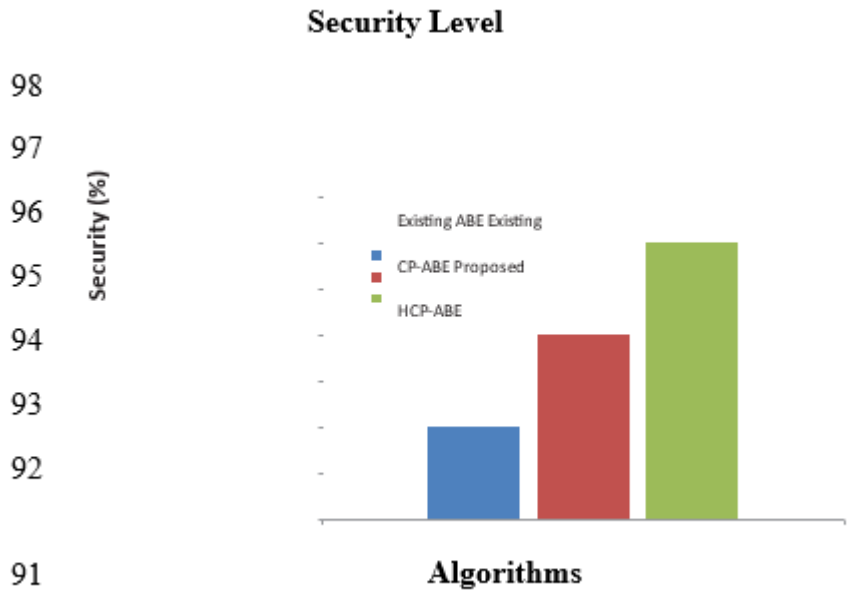


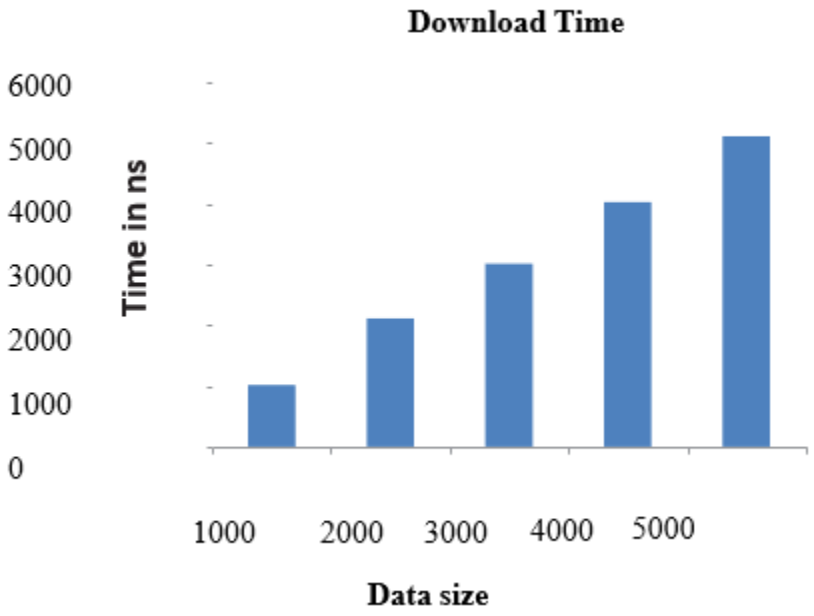
Figure 4: Performance analysis based on the security level

During the data access, the following processes are done that are key generation, cipher text creation, and cipher text verification time. Each process consumes a different time to process. In Fig. 5, the amount of time taken for different processes is analyzed. The figure clearly shows that for the key generation process, 675 ms time is taken, for cipher text creation, 712 ms time is taken, and 824 ms time is taken for the cipher text verification process.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

S



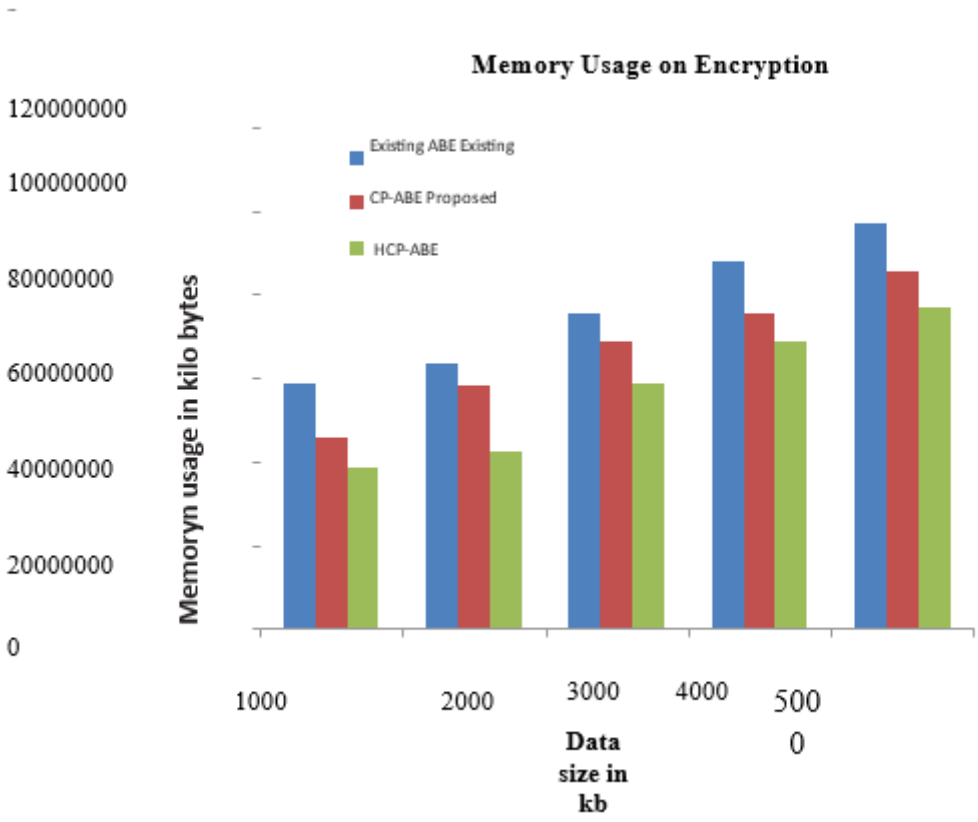
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s

Figure 9: Performance analysis based on download time

Fig. 10 shows the amount of memory usage. To prove the efficiency of the proposed approach, it is compared with different methods. When analyzing Fig. 10, encrypting 5k data, the proposed method utilizes only 76853642-kilo bytes which are 85517741-kilo bytes for CP-ABE-based encryption and 96857874-kilo bytes for ABE-based encryption.



ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s

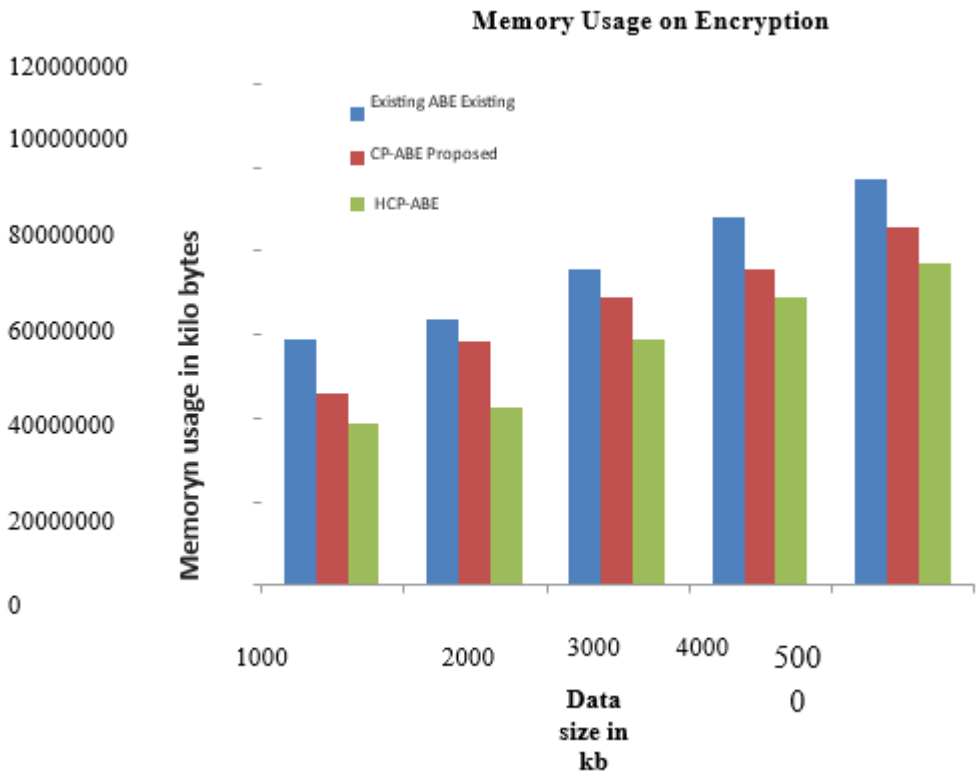


Figure 10: Performance analysis based on memory usage on encryption

Moreover, in Fig. 11, the performance of the proposed approach is analyzed based on memory usage in the decryption process. From the analysis, the proposed method attained better results compared to the traditional CP-ABE and ABE.

3 Conclusion

An efficient HCP-ABE algorithm-based secure data transaction on the cloud has been presented in this work. To prevent the unauthorized login process, an authentication system with a secure access policy has been presented. The access policy has been generated based on the user attributes, mainly location and time attributes. To enhance the system's security, the access policy has been encrypted using the SHA-512 algorithm. The encryption process has been carried out using the HCP-ABE algorithm. The performance of the proposed approach is analyzed based on the different metrics and effectiveness compared with other methods. The proposed HCP-ABE will take 457 ms encryption time and 468 ms encryption time, and those are minimal considering the existing algorithms. Moreover, this proposed work achieves a maximum security level of 97%.

Acknowledgement: The author with a deep sense of gratitude would thank the supervisor for his guidanceand constant support rendered during this research.

Funding Statement: The authors received no specific funding for this study.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Iss 1, 2021

s

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] V. Ratten, "Cloud computing technology innovation advances: A set of research propositions," *InternationalJournal of Cloud Applications and Computing (IJCAC)*, vol. 5, no. 1, pp. 69–76, 2015.

[2] R. Buyya, V. Christian and S. T. Selvi, "Mastering cloud computing: Foundations and applications programming,"
Newnes, 2013.

[3] W. Wu, Q. Zhang and Y. Wang, "Public cloud security protection research," in *2019 IEEE Int. Conf. on Signal Processing, Communications and Computing (ICSPCC)*, Dalian, China, pp. 1–4. IEEE, 2019.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in *2nd USENIX Conf. on File and Storage Technologies (FAST 03)*, pp. 29–42, 2003.

[5] R. Anderson, "*Security Engineering: A Guide to Building Dependable Distributed Systems*," John Wiley & Sons, 2020.

[6] D. E. Bell, "Looking back at the bell-la padula model," in *21st Annual Computer Security Applications Conf. (ACSAC'05)*, Tucson, AZ, USA, IEEE, pp. 15, 2005.

[7] G. Wang, Q. Liu and J. Wu, "Achieving fine-grained access control for secure data sharing on cloud servers,"
Concurrency and Computation: Practice and Experience, vol. 23, no. 12, pp. 1443–1464, 2011.

[8] H. Zhu, L. Wang, H. Ahmad and X. Niu, "Key-policy attribute-based encryption with equality test in cloud computing," *IEEE Access*, vol. 5, pp. 20428–20439, 2017.

[9] X. Huang, W. Susilo, Y. Mu and F. Zhang, "Short designated verifier signature scheme and its identity-based variant," vol. 6, no. 1, pp. 82–93, 2008.

[10] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, Springer, pp. 457–473, 2005.

[11] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Int. Workshop on Public Key Cryptography*, Berlin, Heidelberg, Springer, pp. 53–70, 2011.

[12] Saikumar, K. (2020). RajeshV. Coronary blockage of artery for Heart diagnosis with DT Artificial Intelligence Algorithm. Int J Res Pharma Sci, 11(1), 471-479.

[13] Saikumar, K., Rajesh, V. (2020). A novel implementation heart diagnosis system based on random forest machine learning technique International Journal of Pharmaceutical Research 12, pp. 3904-3916.