International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# A Novel Digital Mark CP-ABE Access Control Scheme for Public Secure Efficient Cloud Storage Technique

**Arvind Kumar Pandey [1], Dr.D.Arivazhagan [2], Sagar Rane [3], Sita M Yadav [4], Khan Vajid Nabilal [5], Dr.Ashish Oberoi [6]**

**Submitted:** 03/11/2022 **Revised:** 13/01/2023 **Accepted:** 02/02/2023

**Abstract:** Daily data outsourcing by cloud users has led to enormous amounts of data being stored in cloud servers. The cloud service provider (CSP) may choose to change the data, which causes a problem with data integrity. The information saved on a cloud server is illegally accessed by unauthorised users. This study suggests a novel approach to cloud storage for big data access control utilising CP-ABE Access Control Scheme, in which the proxy server updates ciphertext as well as secret key upon revocation instead of the data owner and user. Using an algorithm and a key, encryption transforms readable text into unintelligible form. According to the simulation results, the proposed technique performs better in terms of accuracy, precision, F-Score, AUC, and recall when compared to state-of-the-art method. The proposed method achieved 98% accuracy, 85% precision, 74% recall, a 63% F-1 score, and an AUC of 70%.

***Keywords:*** *Cloud server, Cloud service provider, cloud storage scheme, proxy server, Encryption.*

## 1. Introduction

The next-generation of distributed/utility computing has been described as cloud computing. It is described as a model for providing simple, on-demand network access to a shared, configurable pool of computing resources that can be swiftly provisioned as well as released with little management work or service provider involvement [1]. According to National Institute of Standards and Technology (NIST), there are five key criteria, 3 service methods and four deployment types that characterise CC [2]. Private, public, community, and hybrid cloud deployment types are available. These days, the cloud computing paradigm may provide any type of service imaginable, including online services, social networking, telephony, and computational resources for high performance computing applications. Users may also find cloud storage in data centres beneficial for remotely storing and accessing their data from any location at any time with no additional hassle. Security is the main issue with cloud data storage. The cloud device's constant data transmission and reception make it susceptible to a number of attacks. As a result, cloud servers and resources face a greater threat. IDS is integrated into cloud networks to monitor traffic and find malicious activity [3].

## 2. Related Works

Although there has been a lot of research on deep learning, the authors credit the following papers as having had a big influence on this particular study. After land, sea, and air, the cyberspace is regarded as a realm worth exploring and researching [4]. The intermittent rise in cybercrimes and cybercriminals is primarily to blame for this [5]. The development of technology and the Internet has caused an increase in cybercrimes. The most often reported crime, according to Ref. [6], cybercrime is expected to cost $6 trillion in damages globally. According to information security timelines and statistics, cybercrime accounts for 81.7% of attack reasons. Microsoft has also discovered that an attacker may stay on a network unnoticed for an average of 146 days [7]. This demonstrates that network domains, which make up a significant portion of the cyberspace, are where cybercrime attacks are most common. Additionally, cybercrime can take many various forms, and an adversary may employ a variety of methods. Work [8] has categorised cybercrime using the following methods: credit card fraud, phishing, bots, DDoS, virus

[1] *Assistant Professor, Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand India.*
*arvind.p@arkajainuniversity.ac.in*
*0000-0001-5294-0190*
[2] *Professor, AMET Business school, Academy of Maritime Education and Training, Deemed to be University, India.*
*prof.arivazhagan@ametuniv.ac.in*
[3] *Associate Professor, Computer Engineering, Army Institute of Technology, Pune, India.*
*sagarrane@aitpune.edu.in*
*0000-0003-0827-3233*
[4] *Assistant Professor, Computer Engineering, Army Institute of Technology, Pune, India.*
*syadav@aitpune.edu.in*
*0000-0001-9510-4336*
[5] *Associate Professor, Computer Engineering, KJ College of Engineering and Management Research, kvajid12@gmail.com*
*0000-0002-0999-9776*
[6] *Professor, Department of CSE, RIMT University, Mandi, Gobindgarh, Punjab, India.*
*ashishoberoi@rimt.ac.in*
*0000-0003-1451-6684*

distribution, child pornography, cyberstalking, botnets, and software piracy. Cybercrime has gained international attention recently as a subject that presents unique difficulties and can be committed by state or non-state actors [9]. However, study by Ref. [10] has demonstrated that data mining methods can be utilised to recognise cyber-based threats.

## 3. System Model

This section discusses a novel method for controlling access to huge data stored in the cloud using the CP-ABE Access Control Scheme, in which proxy server updates ciphertext as well as secret key during revocation instead of the data owner and user. Using an algorithm and a key, encryption transforms readable text into unintelligible form.

Data Owner. It releases data objects to cloud storage server after encrypting them in accordance with his or her access control settings. Additionally, he/she bases the definition of the SDS limitations on Definition 1 and Rule 1. User. On the cloud storage server, the user has access to encrypted data items.

Key Generation Center (KGC). For system, the KGC creates both public and private keys. It is regarded as somewhat trustworthy. The KGC carries out the proper responsibilities that have been delegated to it by other entities, but it has ability to peek at data objects, access control rules, and constraint policies of data owner.

Proxy Server. The proxy server performs partial decryption and implements access control for data objects. It is regarded as somewhat trustworthy. The proxy server carries out legal tasks that have been given to it by other parties, but it has the ability to peek at data objects, access control rules, and constraint rules of data owner. Another presumption regarding the proxy server is that it does not alter any aspect of data object's ciphertext. SDS monitor carries out proper duties placed on it by other parties, but it has the ability to sneak a peep at the data objects of data owner.

SDS Monitor. It monitor applies SDS constraint on data items. It is thought to be reasonably reliable.

Another important presumption about SDS monitor is that it will delete partially decrypted ciphertext if user is likely to transgress any SDS constraint when accessing the relevant data object.

In the suggested approach, players are divided into cooperative and non-cooperative games. In cooperative games, participants on both teams share the same objectives and approaches to attaining cloud security. In non-cooperative games, one player's objective is distinct from and at odds with other players' techniques for maximising benefit. Attackers and defenders in non-cooperative games complete one another, which is the issue. Equation (1), which is presented as follows, mathematically expresses non-cooperative game model (G) as follows:

$$G = \{(D, A)(S_D, S_A)(U_D, U_A)\} \quad (1)$$

Defender and attacker's strategies are denoted as SD and SA in equation above. UD and UA, respectively, are used to represent the defender and attacker payment functions. An optimization approach is used to incorporate evaluation of player strategy produced model into Deep Neural Network (DNN). Two IDS modules, the Signature Detection (SD) and Anomaly Detection (AD) modules, both use whole specified model. Database stores defender's tactics and accompanying attacks for processing. SD assesses database as well as delivers effective and quick results for data security. On the other hand, AD evaluates complex and unknown attacks. Assaults in AD assess any deviations in the behaviour of the incoming traffic or packets and provide a positive signal value for attack. Attacker sets up a network trap by estimating dummy data on the network. Traffic within the secure cloud is valid after the detecting system. Using the notation SD = SD1, SD2, SD3, the attacker and defensive strategies are expressed.

Query phase 1: For any attributes that have been set to the A, it requests secret key. By using the KeyGeneration method, the produces the secret key for specified set of attributes and delivers it to the A. The challenge is that A chooses to give the the two messages M0 and M1. M0 and M1 must both have the same size.

Query phase 2: Similar to query phase 1, the A might ask for additional secret keys from B, and B would act similarly to A in query phase 1. x Speculate: The A must enter the speculative answer of σc (0, 1). When σc = σ, the game is won by A. The advantage of the opponent over winning the game is known as eq. (2)

$$\left(\Pr[\sigma = \sigma'] - \frac{1}{2}\right). \quad (2)$$

SystemSetup(d) → (PK, MSK): A reliable authority runs this algorithm. It takes security parameter d as an input and outputs PK and MSK.

UserSetup(UL) → UID: TA runs this method each time a new user joins system. This method creates a unique user identifier (UID) and adds it to user list (UL). It accepts UL as input and returns updated UL and UID. x Encryption(M, PK, τ) C: This algorithm is used by the data owner. It returns the ciphertext after receiving the input message (M), key (PK), and access policy (τ).

UUpdateKeyGen(UID, UL, RUL, PK, MSK) → upd_keys:

The user update key generation (UUpdateKeyGen) method is executed by the TA each time a user logs out of the system. The user id (UID), UL, revoked user list (RUL), PK, and MSK are taken in as inputs, and update key (upd keys), which includes flag = "USR," ciphertext update key (uk ct).

Attribute update key generation (AUpdateKeyGen) procedure is run by TA whenever the users cancel an attribute.

CTUpdate(C, upd_keys) → Cc: By proxy server, the ciphertext updating algorithm is carried out. It takes the updated key and ciphertext (C) as input and outputs updated ciphertext (Cc).

SKUpdate(S_Key2, upd_keys) → S_Key2c: Proxy server runs the secret key update (SKUpdate) algorithm.

## 4. Experimental Analysis

Model simulation is carried out in MATLAB to confirm and validate the proposed technique. The payoff function and methods are taken into consideration when estimating the suggested technique. The defender gain is constant at between -5,0 and 5, and the defender detection rate is between 0 and 0.99. If the player keeps 5 or is in a resting state, it receives 0 with no benefit, regardless of whether the payer wins or loses. Otherwise, according to the CICIDS - 2017 dataset, the defender has no points to accumulate. The simulation lasts for 120 seconds while taking the competition between the two players into account.

**Table 1:** Comparative analysis for Proposed and existing technique

| Parameters | LDA | SVM | ANN | Encryp_CP-ABE |
|---|---|---|---|---|
| **Accuracy** | 84 | 90 | 92 | 98 |
| **Precision** | 74 | 80 | 82 | 85 |
| **Recall** | 65 | 69 | 70 | 74 |
| **F1_Score** | 51 | 56 | 59 | 63 |
| **AUC** | 61 | 65 | 69 | 70 |

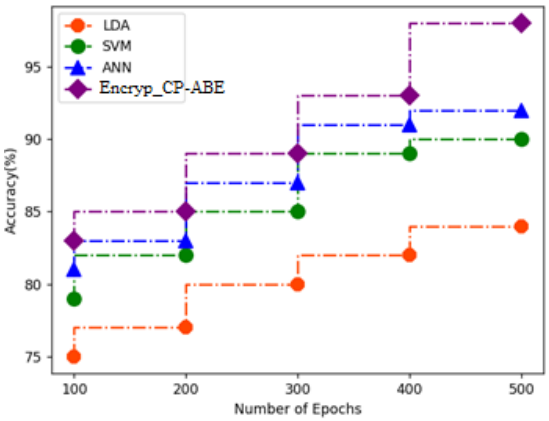


**Fig.-1** Comparison of accuracy

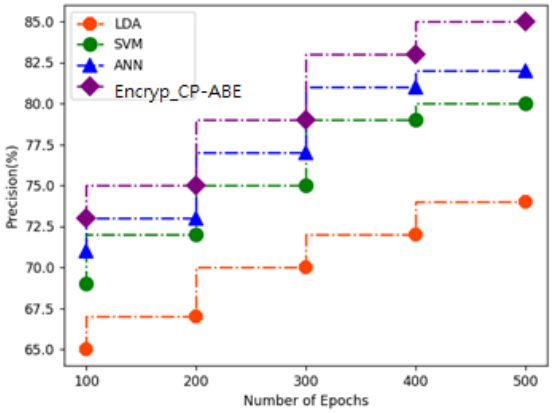


**Fig.-2** Comparison of Precision

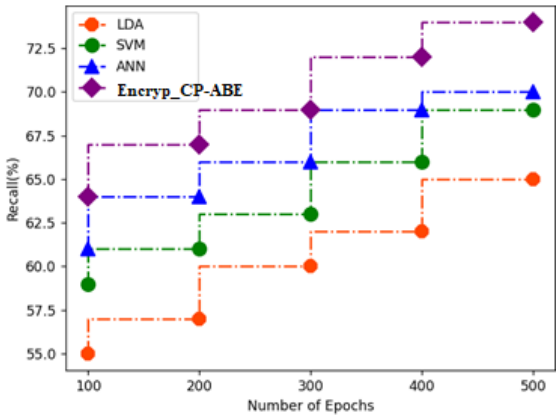


**Fig.-3** Comparison of Recall

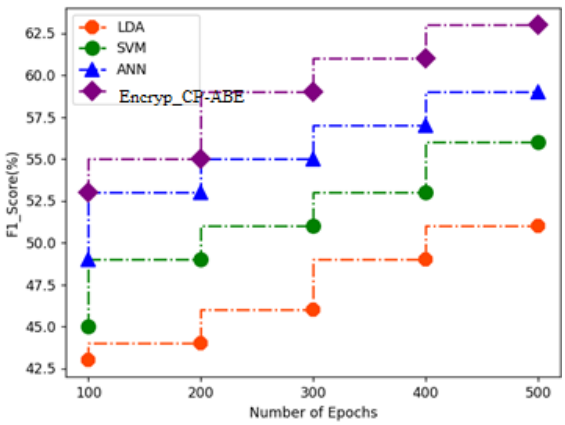


**Fig.-4** Comparison of F-1 score

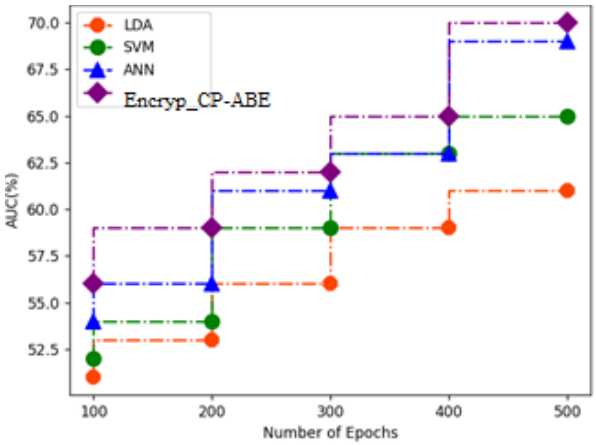


**Fig.-5** Comparison of AUC

Above table-1 and figure 1-5 shows the comparative analysis of cloud based encryption data. Here the comparison has been carried out in terms of accuracy, precision, recall, F-1 score and AUC. Existing technique compared are LDA, SVM, ANN, among which the proposed method obtained optimal results in encrypting the input and cloud control access data. The proposed technique attained accuracy of 98%, precision of 85%, recall of 74%, F-1 score of 63% and AUC of 70%.

## 5. Conclusion

This study suggests a novel method for controlling access to massive data stored in the cloud using the CP-ABE Access Control Scheme. A CP-ABE strategy, however, creates a single-point performance bottleneck when utilised in a large-scale cloud storage system because, in current CP-ABE schemes, single attribute authority is responsible for carrying out time-consuming user validity verification and secret key distribution. Additionally, in our scheme, the Private Key Generator (PKG) may effectively add new users without changing the information that has already been shared.

### Reference

[1] Zhao, J., Liu, L., & Liu, F. (2021, December). Access Control and Anti-copy Scheme of Cloud Storage Data Based on Blockchain. In 2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS) (pp. 622-628). IEEE.

[2] Bhansali, P. K., Hiran, D., Kothari, H., & Gulati, K. (2022). Cloud-based secure data storage and access control for internet of medical things using federated learning. International Journal of Pervasive Computing and Communications, (ahead-of-print).

[3] Liu, S., Yu, J., Chen, L., & Chai, B. (2022). Blockchain-assisted Comprehensive Key Management in CP-ABE for Cloud-stored Data. IEEE Transactions on Network and Service Management.

[4] Yu, Y. (2021, October). Research of Identity Privacy-preserving Scheme Based on CP-ABE. In Proceedings of the 2021 5th International Conference on Electronic Information Technology and Computer Engineering (pp. 695-698).

[5] Sethi, K., Pradhan, A., & Bera, P. (2021). PMTER-ABE: a practical multi-authority CP-ABE with traceability, revocation and outsourcing decryption for secure access control in cloud systems. Cluster Computing, 24(2), 1525-1550.

[6] Singh, D., Sinha, S., & Thada, V. (2021, December). Review of Attribute Based Access Control (ABAC) Models for Cloud Computing. In 2021 International Conference on Computational Performance Evaluation (ComPE) (pp. 710-715). IEEE.

[7] Sammy, F., & Vigila, S. (2022). An Efficient Blockchain Based Data Access with Modified Hierarchical Attribute Access Structure with CP-ABE Using ECC Scheme for Patient Health Record. Security and Communication Networks, 2022.

[8] Zheng, F., Peng, X., & Li, Z. (2022). An Efficient User's Attribute Revocation Scheme Suitable for Data Outsourcing in Cloud Storage. Wireless Communications and Mobile Computing, 2022.

[9] Zhang, J., & Zhang, W. (2021). An Improved FH-CP-ABE Scheme with Flexible Attribute Management and Efficient User Decryption. International Journal of Network Security, 23(5), 856-866.

[10] Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic Health Records Sharing Model based on Blockchain with Checkable State PBFT Consensus Algorithm. IEEE Access.