# An Authentication Model with High Security for Cloud Database


**Krishna Keerthi Chennam, Rajanikanth Aluvalu, and S. Shitharth**

**Abstract** The cloud computing standards are gaining an increased research interest due to various benefits they offer. Though there are so many influences with cloud computing, security and privacy problems are various issues handling with the extensive adaption by the model. Malicious problem of service provider is one more issue which cannot be traceable by data proprietors. Hence, finding the appropriate solutions to these security issues at both administrator level and customer level is very attractive in various directions. Cryptographically enforced access control for securing electronic pathological records (CEASE) is formulated by extending the proposed ciphertext-based attribute-based encryption (CP-ABE) with advanced encryption standard (AES) through limited-shuffle techniques. The main objective of CEASE is to provide data confidentiality, and access control limited-shuffle protects the data from inference attacks and protects the data confidentiality for hot data. In the next step, this research works design a multistage encrypt-or model by differentiating the users as public and personal. Two separate algorithms such as Vigenere encryption algorithm and two-fish encryption are applied in personal and public domain, respectively. Further, where, hierarchical agglomerative clustering (HAC) algorithm is also processed for clustering of users in the public domain by which the overhead decreases effectively. As a final system, this work develops an integrated framework by combining the CP-ABE with AES, multistage encryptor and limited-shuffle. As it is combined with individual methods, this method achieves an efficient performance in the provision of security and data confidentiality.

**Keywords** Cloud computing · Data security · Access control models · Encryption · Clustering algorithm · Limited-shuffle

K. K. Chennam
CSE Department, Muffakham Jah College of Engineering and Technology, Telangana State, Hyderabad, India

R. Aluvalu · S. Shitharth (✉)
CSE Department, Vardhaman College of Engineering, Telangana State, Hyderabad, India



S. K. Das et al. (eds.), *Architectural Wireless Networks Solutions and Security Issues*, Lecture Notes in Networks and Systems 196,
https://doi.org/10.1007/978-981-16-0386-0_2

## 1 Introduction

Cloud computing standards are gaining an increased research interest by the different influences. The major benefit involves time savings, with reduced cost and efficient utilization of computing resources. Though there are so many influences with cloud computing, security and privacy problems are the important problems holding back the extensive adaption of this automation. The general characteristic of cloud computing technology requires the clients to store their data on third-party cloud service providers, which can also be termed as outsourcing of data. The security and privacy are generally maintained by the CSP where the data proprietors do not have complete control on the data security, malicious nature of service provider and third-party users is one more issue which cannot be traceable by data proprietors. Hence, finding the appropriate solutions to these security issues at both administrator level and client level is very important in various directions.

Earlier research is based on standard encryption algorithms like AES, data encryption standard (DES), etc. However, the advancement in the technology makes these approaches ineffective because of the lack of control on authorization and authentication. In contrast, the attribute-based encryption (ABE) was the new research which has the desire to give the maximum to handle by the data proprietors who can give the data and also provide an efficient management for the cloud service provider. However, the ABE-based approaches provide security at the cost of execution. Therefore, the challenge of achieving the dual goals of privacy preserving with effective cloud data sharing remains unresolved.

In summary, the major significant addition in the section is to influence by the benefits of the ABE application to carry out the real-time answers to security and privacy problems experienced in the cloud computing environments.

Section 1 discusses the introduction about cloud computing, data security and access control schema. Section 2 discusses the CP-ABE with AES, Sect. 3 discusses the CEASE, and Sects. 4 and 5 talk about the partial shuffling with two-stage encryption and integration model. Last section discusses the results and conclusion.

## 2 Problems in Data Security

Security, privacy and trust issues are existing and given importance since the evolution of Internet, and they are widely spoken these days because of cloud computing. Cloud's dynamic nature demands higher security levels. Users or organizations subscribed to cloud for running their business processes are strikes to acquiring the next level of endanger because of expanded applications. A cloud user while saving the data on the cloud, which wants to make sure if the data is correctly stored and can be retrieved later. The service provider must ensure the secure infrastructure to protect the data and applications of its clients and the users. Various security strategies proposed earlier have become ineffective due to advancements in technology.

This is not the usual CSP and the user for both imaginations. What is required is a mechanism that assures data consistency to the cloud user and protects that the user is not some malicious hacker. Hence, the necessity for developing trust-based security model is the need of the hour.

## 3 Objectives of Data Security

Cloud computing applications have to ensure security of the data stored in the cloud. Existing approaches are suffering from various drawbacks and require improvement. In particular, the proposed scheme has the following objectives:

(a) Dual optimization: Data confidentiality and processing time are the two main constraints which are not achieved simultaneously. More processing time (encryption time + decryption time) is required to achieve an efficient data security for data stored in the cloud. On the other hand, the less computational operations to encrypt the data will reduce the data confidentiality and result in an information loss. To meet these two constraints simultaneously, this research work focuses on developing an effective cloud computing technique based on the ABE [1] and multistage encrypt-or. By adding some more standard techniques (AES and limited-shuffle) with these approaches, this work tries to achieve the data confidentiality and less processing time.
(b) Increase data confidentiality: To achieve increased hot data confidentiality and preservation of privacy, this work proposes a CEASE. In this approach, an advanced encryption standard accomplishes an encryption algorithm to reduce the effect of curious/malicious administrator.
(c) Resilient to inference attacks: To make the system more secure from inference attacks and from malicious authority attacks, this work proposes a single-level block index method along with limited-shuffle, by which the system acquires data accomplished models off the record without reducing the querying process.
(d) Reduced computational overhead: To reduce the unnecessary computational overhead in the large-scale cloud storages, this work accomplishes a clustering mechanism, called HAC supports based with the place of utilizers.

### *3.1 CP-ABE with AES*

This section proposed access control within database strategy, CP-ABE combined with standard AES algorithm. Here CP-ABE [2] achieves the authenticated accessing of only legal users and AES ensures the data security. Before uploading data to the cloud, it is encrypted through AES algorithm by which the data user will be relaxed about the data security. Further in CP-ABE, proprietor accommodates attributes set, when the user wants the data accomplishment which needs the attributes set and

requires the secret key for decrypting the data, where encrypt-or accommodates the key with the strategy of the access control plan of action. Though administrators are curious about the data, due to the non-availability of key, the data cannot be accessed by that malicious authority [3]. Hence, this method protects the security from malicious authority more effectively [4].

The proposed strategy gives cloud document for the security space with respect to performance metrics like key generation time, encryption and decryption time. The key generation time is computed with various secret keys with the identified set attributes. To produce non-public key in CP-ABE with AES is not exactly the same by CP-ABE with bilinear mapping. It is observed that, for every attributes set, the obtained key generation time is less when contrast to the conventional CP-ABE with bilinear. The encryption time and decryption time are computed with various no. of policy of leaf nodes, which is limited in CP-ABE with AES contrast with CP-ABE with bilinear mapping. CP-ABE with AES gives protection and security for data records for the information of the cipher and store in cloud. The CP-ABE with AES gives limited key generation, encryption time when contrasted by CP-ABE with bilinear mapping.

## 4 CEASE

The CEASE is outlined in this section; main objective of CEASE is to provide data confidentiality and access control of outsourced CS information over the security threats. The proposed CEASE framework comprises three constituents to protect the cloud data security:

(a) Accomplishment of AES on sensitive patient health records.
(b) Secure information retrieval through a data accomplishes and direct technique and query encryption.
(c) Data confidentiality for hot data through limited-shuffle to protect the data from inference attacks.

Initially, the holder of data modifies the loyal proxy server by extending AES on the health data before transferring it to CSP. Ordinal, the proxy server is the important attribute set administration recognizes the individuals applying the set of attributes and overdrives access control plan of action on electronic information inward cloud. The encrypted queries retrieve the encrypted data from the cloud and to decrypt the data using attributes in the proxy server before delivering information to the final consumer. Nevertheless, retrieving encrypted information of ciphertext assures high confidentiality of every patient record in the cloud, and there is a possibility of inference attacks. Thirdly, the CEASE techniques apply the limited-shuffle within a single block of the data that contains the sensitive health records and protects the data confidentiality aside from swift retrieval. Thus, the recommended CEASE algorithm protects malicious authority of cloud unable to take or change (hot) information one of two is treasure delicate health files or encrypted query execution along with the

faster querying process [5]. The performance metrics such as querying cost, storage overhead and hot data confidentiality are examined on the recommended method. The decryption algorithm decrypts the data and sends the plain text to the client when the set of attributes are matched according to the CP-ABE with AES.

The performance evaluation of recommended CEASE is carried out on the JAVA platform on a personal health records. The performance metrics such as querying cost, storage overhead and hot data confidentiality are measured for varying data sizes. From the simulation results, it is proved that the recommended approach shows slight increase in the querying cost but reduced storage overhead and finally an improvement in the hot data confidentiality contrast with existing approach.

Algorithm 1 Decryption algorithm

**/*Decryption Algorithm*/**

**Input**: A CT block $\{CT_1, ..., CT_k\}$ and keys$\{K_{att1}, ..., K_{attk}\}$

**Output**: Plain-Text

1: **Assign** k=1 and i=|CT|

2. **If** k$\leq$|CT| **do**

3. **for** each k **do**

4: **execute** equation (4.2)

5: **Assign** k=k+1 and i=|CT|-1

6: **else**

Plain-Text = $PT_k$

## 5 Multistage Encrypt-Or for Securing Data Records

This section outlines the recommended multistage encrypt-or strategy of protecting the personal health records (PHR) of third-party database storage. The main objective of this approach is to provide security for the PHR in the cloud with less computational overhead. The framework differentiated by the multiple regions partitioned by public and personal domains is discussed according to the client's data to give access permissions.

To ensure security in the non-public domain, this approach uses Vigenere encryption algorithm, and for the public domain, it uses the two-fish-based encryption algorithm. For every user in the non-public domain (PSD), the clients, relatives or nearby people are connected in a chain fashion, and they are able to get PHR in glimpse of

getting opportunities designated from the sick person. Here each client achieves the Vigenere encryption-based system to manage the decoding by receiving awards of customers in his/her PSD. In public domain (PUD), two-fish encryption is used by the attendant of diverse AAs, each one directing a disjoint subset of characters [6, 7]. To regulate approaches by the PUD wards and let on to reflect role-oriented fine-grained approaches for their PHR documents, while they do not require the sanctioned users at the time of encryption. The PUDs contain the maximum number of wards. By coming through the difficulty, here this approach groups the ward's duty in the PUD with HAC algorithm. Wards of PUDs get back attribute designated encryption keys supported with the ward functions. The observational maps about encryption, decryption time, clustering accuracy and storage requirements are evaluated using various data set sizes. The observational effect shows that the recommended method has more clustering quality, less encryption and decryption time.

## 6 Raising the Security with Fine-Grained Access Control Plan of Action Using Two-Stage Encryption with Limited-Shuffle in the Cloud

This section integrates the CP-ABE with AES and two-stage encrypt-or with limited-shuffle [8]. The primary goal of CP-ABE with AES is to recognize the malicious clients and data proprietors who can access data from the cloud. Next, the multistage encrypt-or helps in reducing the extra computational overhead [9]. The electronic records are protected from inference attacks by applying limited-shuffle as shown in Fig. 1. The data proprietors are maintaining the keys distribution authority, certificate verification and attribute authority and send the data to the proxy server. The proxy server applied two-stage encryption techniques based on the domains mentioned above, while doing encryption the key pairs are received from elliptic curve. The encrypted data is stored in the cloud database. The proxy server encrypts data before storing in cloud and plain queries also encrypted by proxy server before retrieving data from cloud, where there is no possibility of plain data to the malicious admin in cloud and in network or in proxy server.

Two-fish algorithm uses with different and random key length of variable size of 128 bits, 192 bits and 256 bits. Two-fish is a symmetric algorithm with quick encryption great with AES due to its speed, adaptability and protection outline. For every query, the database needs to be searched line by line in the table, where the questioning time is expanded as the information size is expanded straightly. To address this issue, a record is made by information by examining the file is decent as opposed to examining the entire information base. The entire information base records are organized consecutively with the Customer ID. Before storing new data into database by examine place by identification and a short time later by embed new segment with the objective that masterminding demand should be kept up. Single-level information square relies upon activity key, and the information is kept in

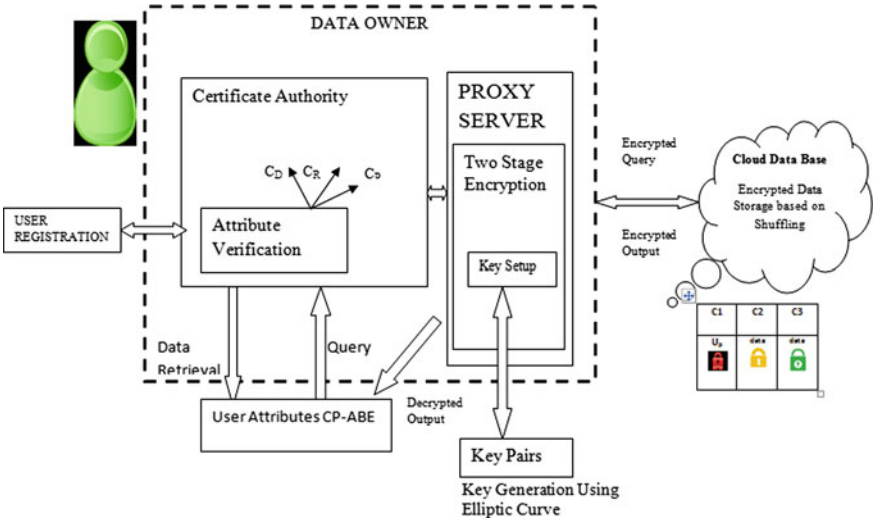


**Fig. 1** Proposed methodology

squares. All information kept in the database is named as transparent record. Right when the record is recovered from the information base, the information is changed to dark. The flooded list rearranging is not required where transparent stamped records are not recovered, and it is highly unlikely of spillage with transparent records. Dark checked information is revamped high for entire single list information base after each rearranging is finished. By rearranging the dark records is a constrained mix strategy with the different information squares which outfit information mystery and brisk questioning with the ordering [10, 11].

Protecting the pathological information initially by the access control plan of action is used based on the user attributes which is CP-ABE and the information is encrypted [12] by AES techniques by separating the security domain into multiple areas one is non-public domain and another is public domain where cardinal-independent encryption schemes are used for different domain, one is Vigenere encryption used for non-public domain, and two-fish algorithm is used for PUD, respectively, as shown in Fig. 2. The chance of information spillage of third-party database provider of regular avenue example of records, to beat that the restricted mix, is utilized with single square stockpiling and high security is given with the method [13]. This strategy includes less key generation time, encryption time and unscrambling period much as appeared differently in relation to spare CP-ABE plans, eventually, centered on the distinctive encryption calculation to make sure about pathological information.

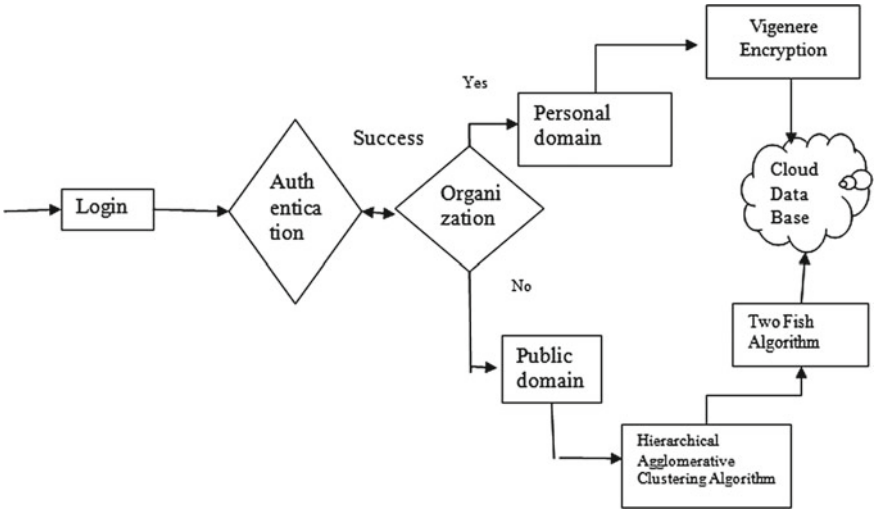


**Fig. 2** Multistage encrypt-or

## 7 Result Analysis

This section outlines results of the recommended schemes on the personal health records (PHR). The entire recommended methodology is accomplished over the PHR data set, and its performance is evaluated through the performance metrics such as encryption time, decryption time, time taken to generate non-public key and hot data confidentiality [14].

The overall research work is implemented in four phases to meet the defined objectives.

1. Dual optimization through hybridizing CP-ABE and AES.
2. CEASE—Improving data confidentiality and developing resistance to inference attacks through hybridizing CP-ABE, AES and implementing limited-shuffle.
3. Multistage encryption—Reduction in computational overhead by using multi-stage encryption on hybridized CP-ABE with AES.
4. Integrating the multistage encryption model with limited-shuffle to further reduce the computational overhead [15].

The information is scrambled before re-appropriating onto the cloud with symmetric encryption using AES. This mechanism will restrict the unauthorized users from accessing the data, and the administrator cannot decrypt the data as they are not given access to keys. By utilizing this recommended model, the information is made sure about AES encryption and CP-ABE containment strategy. CP-ABE with bilinear mapping is in contrast to CP-ABE with AES on different parameters. The key age time is decreased utilizing the recommended system. It is seen that CP-ABE with bilinear mapping is procuring tremendous time to generate key than

the CP-ABE with AES. The plain information is scrambled before re-appropriating the information in cloud to shield the information from the pernicious manager. The encryption time is diminished in CP-ABE with AES in contrast to CP-ABE with bilinear mapping and KP-ABE. The customer needs to unscramble the information, and the decoding times for CP-ABE with AES are lessened in contrast to the CP-ABE with bilinear mapping and KP-ABE. Ciphertext varies less and has more safety measures in both recommended and existing techniques. Furthermore, the recommended CEASE calculation makes sure that the vigorous admin of third-party database cannot recover any (hot) information from the delicate records.

The CEASE scheme enforces the recommended method performance. This method is resolved by various levels in the access control plan of action, encrypted database to store in third-party database and limited-data shuffling. The performance of CEASE scheme is in contrast to the encryption scheme integrated with an access control (EIAC). Querying cost is defined as the time taken to fetch the query result against encrypted database, data encryption and decryption time. The querying cost is slightly increased with the database size, but the storage overhead is less and hot data confidentiality is in more contrast to the existing methods.

Thirdly multistage encrypt-or model is tested on the personal health records. As the number of users on the public domain may be high, securing the data access is a complex issue. Hence, two-stage encryption model is developed. For a user located in the personal domain, this approach adopts Vigenere encryption algorithm, and for a user located in the public domain this approach adopts two-fish encryption algorithm. For each personal domain, the data proprietor is connected in a chain fashion through his/her generations and dear one, which may retrieve personal records in view of access given by the data proprietor. Here every data proprietor uses Vigenere encryption algorithm, maintains the decrypting key and requires sanctions of his/her wards in his/her personal. The key generation is completely carried through the elliptic curve method. The generation of key pairs is only allowed after the authentication of the user.

In the public domain, the users are clustered through HAC algorithm. Based on the roles and responsibilities of the users, they are clustered into some groups in a hierarchical fashion. Finally, the performance is measured through the performance metrics such as encryption time, decryption time, storage requirement and clustering accuracy for varying data sizes.

Multistage with two-fish and Vigenere encryption is in contrast to the existing blowfish algorithm. Further the multistage method is evaluated through clustering accuracy. Here the clustering accuracy is measured as the number of users grouped into public and personal domains. Since the clustering also plays an important role in the security provision, the performance of recommended approach is measured by varying the data size, and for every instant the clustering accuracy is measured and formulated. Two-fish and Vigenere encryption and decryption time are in contrast to the existing blowfish algorithm, and results are tabulated [16, 17].

Finally, an integrated approach using CP-ABE with AES and multistage encrypt-or exhibited high performance through limited-shuffle. The final model is constructed by merging the CP-ABE with AES, multistage encrypt-or and limited-shuffle. The

main objective of CP-ABE with AES is to perceive the malicious clients or administrator and not giving access for unauthorized users to analyze the data in the cloud. This has demonstrated that the recommended strategy encryption time and unscrambling time are not exactly the other CP-ABE plans. To encode the information before outsourcing by isolating the PUD and PSD, encryption is diminished, comparably unscrambling time likewise decreased in this recommended strategy.

In key generation time, secret keys with various numbers of set of attributes which match the equivalent sets based on the leafy nodes, and the keys are generated as shown in Fig. 3. Figures 4 and 5 show the encryption and decryption time for various database sizes, respectively, with the matched attributes sets. Figure 6 shows the

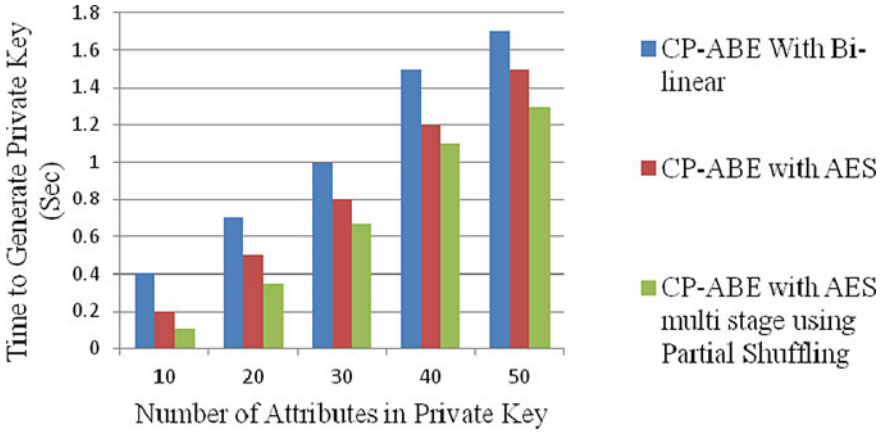


**Fig. 3** Key generation time (MS)

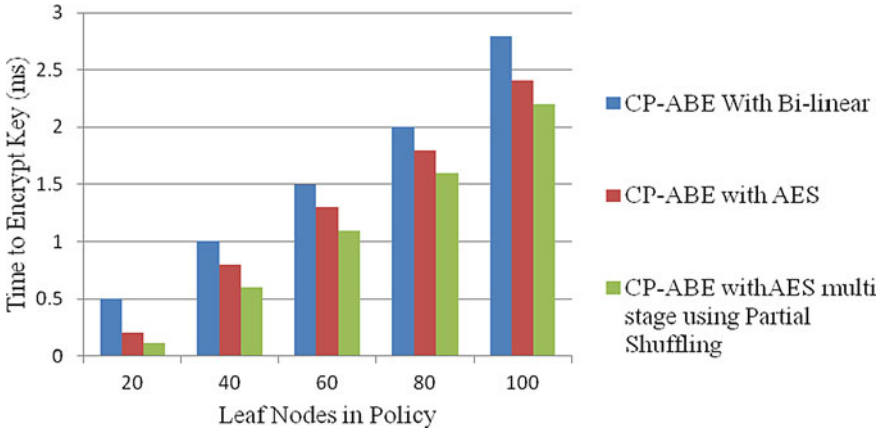


**Fig. 4** Encryption time (MS)

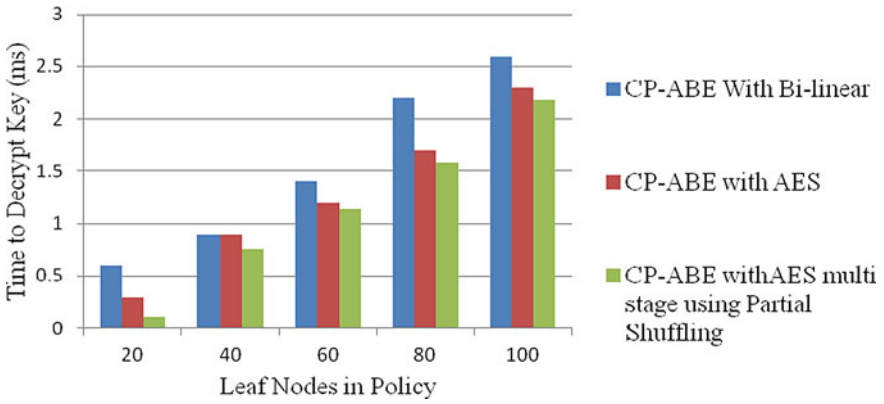


**Fig. 5** Decryption time (MS)

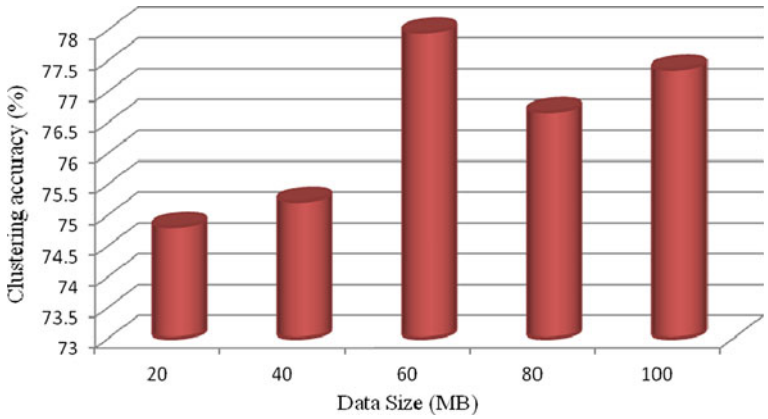


**Fig. 6** Data size versus clustering accuracy

clustering accuracy for different database sizes with HAC algorithm. The multi-stage encrypt-or helps in reducing the additional computational overhead which is acquired by separating all users into clusters. This methodology endeavors to shield the electronic records from inference attacks through the accomplishment of limited-shuffle [18, 19]. The key generation and information retrieval time are limited in the developed model in contrast to various CP-ABE and KP-ABE techniques.

## 8 Conclusions

This considered the implementation of CP-ABE with AES and two-stage encrypt-or exhibiting high performance through limited-shuffle. In this work, initially CP-ABE

with AES is developed and proved reduced key generation time. Secondly, CEASE is developed to use query encryption method to retrieve results from database. Thirdly, multistage encryption model using two-fish and Vigenere is developed.

Here the users are divided into non-public and public domains, and HAC clustering is used to further divide the users into groups. This work is evaluated by performance metric and clustering accuracy [20]. Performance of HAC approach is also measured by varying the data size for every instance. Finally, the integrated model is developed using CP-ABE with AES and multistage encryption model through limited-shuffle. Final work will endeavor to shield the electronic records from inference attacks through the accomplishment of limited-shuffle. This model has majorly addressed the below challenges, namely dual optimization to meet the equality between the data confidentiality, and processing time is achieved with AES and limited-shuffle-based ABE. Increased hot data confidentiality and privacy preservation are achieved by reducing the effect of curious/malicious authority using an encryption algorithm CEASE. Resilient to inference attacks from malicious authority is attained by information access arrangement familiarity by not changing the querying process using single-level block index method along with limited-shuffle. Reduced computational overhead to reduce the unnecessary computational overhead is achieved by HAC algorithm mechanism based on the roles of users. Future work is to reduce the cost of recommended model by increasing the security in data.

**Acknowledgements** Thank you for your cooperation and the contribution of co-authors and Springer for publishing the manuscript.

## References

1. Lewko A, Waters B (2004) Decentralizing attribute-based encryption, EUROCRYPT, pp 223–238.
2. Waters B (2011) ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, public key cryptography–PKC. Springer, Berlin, pp 53–70
3. Boneh D, Boyen X, Goh EJ (2005) Hierarchical identity based encryption with constant size cipher text. Advances in cryptology—EUROCRYPT vol 3493, pp 440–456
4. Bettencourt J, Sahai A, Waters B (2003) Ciphertext-policy attribute based encryption. In: IEEE Symposium on security and privacy (SP), pp 321–334
5. Bobba R, Khurana H, Prabhakaran M (2009) Attribute-sets: A practically motivated enhancement to attribute-based encryption. In: European symposium on research in computer security, pp 587–604
6. Chase M (2007) Multi-authority attribute based encryption. Spring Theory Cryptograph 4392:515–534
7. Ferretti L, M Colajanni, M.Marchetti (2013) Access control enforcement on query-aware encrypted cloud databases, IEEE 5th international conference on cloud computing technology and science (CloudCom), vol 2, pp 219–219
8. Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security, ACM, pp 89–98
9. Muller S (2008) Distributed attribute based encryption. J Inf Secur Cryptol 4:20–36

10. Mell P, Grance T (2011) The NIST definition of cloud computing. National Institute of Standards and Technology Special Publication. 53:1–7
11. Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Advances in cryptology, EUROCRYPT-2005, Springer, pp 557–573
12. Muller S, Katzenbeisser S, Eckert C (2009) On multi-authority ciphertext-policy attribute-based encryption. Bull Korean Math 46(4):803–819
13. Chennam KK, Muddana L (2018) An efficient two stage encryption for securing personal health records in cloud computing. Int J Serv Oper Inf 9(4):277–296
14. di Vimercati SD, Foresti S, Paraboschi S, Pelosi G, Samarati P (2014) Protecting access confidentiality with data distribution and swapping. In: Proceedings of IEEE 4th international conference on big data and cloud computing (BDCLOUD), pp 167–174
15. Yang K, Zhang J, Zhang W, Qiao D (2011) A light-weight solution to preservation of access pattern privacy in un-loyal clouds. In: Proceedings of the European conferences on research in computer security (ESORICS), pp 528–547
16. Wan Z, Liu J, Deng RH (2012) HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. IEEE Trans Inf Forensics Secur 7(2):743–754
17. Hao R, Yang H, Zhou Z (2019) Driving behaviour evaluation model base on big data from internet of vehicles. Int J Ambient Comput Intell 10:78–95. https://doi.org/10.4018/IJACI.2019100105
18. Chandrakar P (2019) A secure remote user authentication protocol for healthcare monitoring using wireless medical sensor networks. Int J Ambient Comput Intell 10:96–116. https://doi.org/10.4018/IJACI.2019010106
19. Das SK, Samanta S, Dey N, Kumar, R (2020) Design frameworks for wireless networks, lecture noted in network and systems, Springer.
20. De D, Mukherjee A, Kumar Das S, Dey N (2020) Nature Inspired computing for wireless sensor networks. Springer Tracts in Nature-Inspired Computing, Springer.