Attribute-Based Encryption for Fine-Grained Access Control on Secure Hybrid Clouds

Sridhar Reddy Vulapula[1]
Research Scholar- KLEF, Vijayawada, A.P. India

Srinivas Malladi[2]
Professor-KLEF, Vijayawada, A.P. India

***Abstract*—In the present scenario, the proliferation of cloud computing services allows hospitals and institutions to move their healthcare data to the cloud, enabling global access to data and on-demand high-quality services at a lower cost. Healthcare data has sensitive attributes to be shielded from leakage due to inference attacks by a curious intruder, either directly or indirectly. A hybrid cloud is a mix of both private and public clouds proposed for the storage of health data. Carefully distributing data between private and public clouds to provide protection. While there has been ample work for the delivery of health data for some time now, it does not appear to be more effective in terms of both data retrieval and consideration for fine-grained access control of the data. This work suggests a cordial approach for a more reliable delivery of data using geometric data disruption of health data over hybrid clouds. It is focused on an in-depth review of the results. The distribution enforces fine-grained data access control using attribute-based encryption. In addition, the approach also addresses a method to effectively extract relevant information from hybrid clouds.**

Keywords*—Secure hybrid cloud; geometric data perturbation; efficiency; fine-grained access control; attribute-based encryption

I. Introduction

Recently, many organizations have been in the process of converting data management to cloud storage in the light of factors such as cost-effectiveness, affordability, redundancy, etc. [4]. The use of cloud computing in healthcare companies enables the exchange of inter-organizational medical data. Data protection and privacy are the two most critical things to remember when it comes to cloud data storage. Possible leakage of confidential medical data could compromise the privacy of the person [1]. While encryption methods are used, leakage of sensitive data can still occur by inference, likely contributing to anti-social activities such as extortion, defamation, etc. It is therefore of utmost importance to ascertain the protection and privacy of data stored in the cloud. All approaches currently used for the defense of privacy can be classified as follows:

- Anonymization.
- Randomization.
- Cryptographic techniques.
- Diversification.
- Aggregation.

However, these approaches have some deficiencies related to the size of operations. Lately, hybrid clouds have been brought forth by many to improve security and privacy [3]. The data is obfuscated or transformed by using specific parameters. The obfuscated data is stored in the untrusted public cloud while the completely trusted private cloud is used to store the parameters used for obfuscation. Through transmitting obfuscated information and parameters used for various data stores, the confidentiality of the obfuscated data is guaranteed even when it is leaked. Certain open issues related to cloud-based hybrid storage solutions are listed here:

- Efficiency in storage and retrieval process.
- Fine-grained access control on the data.

The differential handling of the protection of attributes must be based on the degree of sensitivity. Besides, the fine-grained access control must be carried out for various classes of users. The disrupted data must be indexed for efficient retrieval. The retrieval method must also be secured from inference attacks. In addition to data security, the index must also be protected as private information may be accessed by inference. With these criteria, a stable geometric data disruption approach for health data using hybrid clouds is proposed in this work. The perturbation is controlled through attribute-based encryption [2]. The method also proposes a fine-grained access control on perturbed data with efficient secure indexing and retrieval of information.

II. Related Work

Authors in [1] suggested a novel means of inter-organizational data exchange for health data. The solution is designed to address the protection and privacy needs of patient data for semi-trusted clouds. Encryption dependent attributes were proposed for limited access in this work. Data distribution through several clouds is achieved by cryptographic hidden sharing [26]. Retrieval of the required data is becoming slightly inefficient in this approach due to the presence of more cloud service providers. A scalable data anonymization technique is proposed in [2]. A proximity privacy model dealing with the semantic proximity of sensitive values and multiple sensitive attributes is proposed to resolve privacy breaches. Proximity-aware agglomerative clustering algorithm groups similar records into hierarchical groups and differential privacy is proposed for these groups. Encryption based attributes (ABE) is used to enhance the security of electronic health records in [3][28]. With the use of ABE, the two-fold benefit of reducing connectivity costs and fine-grained access control is achieved. The authors evaluated the performance of four different ABE systems – CP-ABE, KP-ABE, HABE, DABE. Authors in [4] suggested a solution

to ABE's main distribution problems when used to protect electronic health records in the cloud. Besides, the key distribution method is often streamlined by using attributes and implicit authentication. The scheme is based on the premise that a centralized main issue of authority becomes an obstacle to failure. Encryption based attributes and searchable encryption are suggested for retrieval of fine-grained information-based keywords in [5]. It is a multi-authority scheme and the user hidden key distribution is proposed to solve the problem of key leakage. This scheme is successful for resource-restricted devices and most appropriate for fog computing nodes. A hybrid approach to protecting data sharing in the cloud for privacy is proposed in [6]. Authors in [7] used a reversible Privacy Contrast Mapping (RPCM) algorithm to disrupt info. The algorithm involves two phases of data destruction and data recovery. Perturbation is accomplished by grouping together two adjacent data values. In addition to embedding a watermark, this is accomplished. The troubling data is being restored at the recovery stage. An embedded watermark is used to verify the quality of the data being disturbed. A fast-disrupting tree structure algorithm is proposed in [8]. Disruption time is reduced by using a particular tree-crossing technique using specified tree and table structures [9]. Fuzzy keyword search is suggested along with fine-grained access control of encrypted data. The author also recommended that ABE be moved to the private cloud to reduce the cost of computation at the end of the customer. The Privacy Protection Data Publishing System, called the Hybrid Clouds Cocktail, is proposed in [10]. An Expanded Quasi-Identification-Partitioning (EQI) technique is proposed for the partitioning of data during the data publishing process. The differential privacy technique is used at the level of the data question to protect against infringements of privacy. In addition to reducing the loss of information, this strategy also requires data security. The implementation of an independent data partition strategy is suggested in [11]. Relevant data is stored in a private cloud while the public cloud includes disrespectful data in this scheme. Authors in [12] proposed a two-stage data interruption scheme called RG+RP. The user disrupts data using a non-linear Repeated Gompertz (RG) and then projects data to a lower dimension in a distance-preserving manner using a random project matrix (RP). The use of this two-stage scheme avoids the loss of data due to estimation attacks and independent component analysis attacks. Due to distance preservation, fuzzy c mean clustering can be performed on disrupted data with the same result as that applied to raw data. An assault of resilient geometric data disturbance is proposed in [13] [14]. In this thesis, a multidimensional geometric perturbation method called random disturbance projection is proposed. Authors in [15] suggested rapid indexing for data retrieval in a stable cloud. Compression sensing is used for sampling, compression, and recovery of data. To retrieve data, an encrypted high-performance index is created. A new method of anonymization, which is protected against an attack on identity disclosure, is proposed in [16]. The scheme translates data into fixed intervals and then replaces the original values with the averages. The transformation of data is one way and cannot be restored to the original state. An anonymization scheme based on the data classification capability is proposed in [17]. The data classification capacity is calculated using shared knowledge. Two K-anonymity algorithms are proposed to transform the data without losing the ability to distinguish. A privacy protection system for association rules data is proposed in [18] [19]. Combined clustering and geometric data disturbance approach to enhancing the privacy of health data in hybrid clouds [20] [21] using the GDP algorithm, which separates data using K-means, making it difficult to identify. Higher entropy attributes are viewed as sensitive and transformed. Authors in [22] [23] proposed a system by which Cloud Service providers could deal with the protection of information provided by remote clients in the cloud. Furthermore, protection can be given to the general public in this application without understanding it personally. The client's confidentiality is done in this way. In this document, Hash Counter Hash (HCH) is the latest protection offered by the suppliers of the administration, and the information is accepted by the information owners, who have finally scrambled the information demanded by the clients and unscrambled the information for use. A modern decentralized approach to access control in [24] is implemented, i.e. Scalable Attribute-Based Encryption (SABE) to achieve versatile and scalable access control in cloud computing for safe cloud storage. SABE not only performs scalable due to its pyramid structure, but also shares powerful and versatile access control support for ABE, it also assigns user expiry and revocation time efficiently to existing schemes. Thus, in this paper, we propose and build Transmitted Team Key Management (TTKM) where each client (user) in the community shares a hidden trust key owner with subsequent re-keying for data sharing through entering or leaving users' needs only broadcast messages between data sharing in the cloud. We evaluate the privacy of the proposed TTKM scheme and compare it to the current SABE protection scheme for distributed data sharing. Experimental findings showed successful regulation of data access with security considerations. Writers of [25] projected how to provide protections for data stored in the cloud. Data stored in the cloud can be either public data requiring minimal protection or extremely sensitive data requiring high protection. We evaluate the privacy of the proposed TTKM scheme and compare it to the current SABE protection scheme for distributed data sharing. Writers of [25] projected how to provide protections for data stored in the cloud. Data stored in the cloud can be either public data requiring minimal protection or extremely sensitive data requiring high protection. This can be achieved by authenticating the client. In addition, there are a range of similar security and privacy concerns that fall under two broad categories: security and privacy concerns faced by cloud providers and their customers. With the available algorithms that are used to convert plain text to cypher text, apply the principle of steganography to the cypher text and make protection more effective and protect data from unauthorized access. We need a reliable framework to resolve security concerns at the time of data processing in the cloud. As a result, authors in [26] trying to find the best method for accessing cloud data by comparing all attribute-based encryption, such as KP-ABE, CP-ABE and HASBE, addressed the different features of these ABE systems by discussing all features of these schemes

in a tabular manner. Features such as Access Policy, Attributes Fine graininess Access Control, Overhead Computation, Performance, User Revocation, Scalability, and Collision-Resistance were addressed in depth, including Advantages and Limitations. It is suggested in the [27] Biometric Access Scheme that specifies that the biometric data is encrypted and submitted to the cloud server. In which biometric access is encrypted, database providers can then send data to the cloud. Cloud performs some encrypted database operations to send to it and returns the output to the database owner. Security analysis shows that the scheme is protected even though attackers try to target the database and want to access the data of users present in the cloud. Compared to the other protocols, the results inform us that the scheme has achieved better efficiency. Authors in [28] proposed a CSHQS (Cloud Protection Hybrid Querying System) algorithm that efficiently processes data security in a hybrid cloud, and that sub-query framework handles different components.

III. Searchable Fine Access Control on Secure Hybrid Clouds (SFAC-SHC)

The architecture of the new Secure Hybrid Cloud Fine Access Control (SFAC-SHC) is shown in Fig. 1. The suggested solution includes the following steps:

- CP-ABE based key generation.
- Fine-grained access control.
- Geometric perturbation.
- Secure Retrieval.

A. CP-ABE based Key Generation

Of the four-basic setup, key generation, encryption, and decryption algorithms, only two stages of setup and key generation are used in this work. The key authority or generation center produces both public and private keys. When the data owner uploads the file, the key authority needs a policy of access for each user in terms of attributes to the key authority. The qualified key authority shall produce a single public and private key for each access policy. The public key / private keys corresponding to the policy are sent to the data owner and the private key is given to the corresponding data users when the information is requested.

The access policy used in this work consists of two sets of information:

1) Attribute – value pairs of the user

2) Fields or Column names in the dataset allowed for view for the user.

The key generation is based on the policy attribute-value pairs. The file or column name for access is managed by the fine-grained access control point.

B. Fine-Grained Access Control

The health care dataset uploaded by the data owner is a table format for each patient row and each column is a field. The dataset (Table I) has three classes of information: Class 1, Class 2 and Class 3.

The data owner encrypts Class 1 information with the public key obtained by the key authority using any symmetric key algorithm and generates a processed data set. Each row has an identifier that can be either a unique string or a number.

An association map is created between the policy private key and the field or column names permitted to be accessed by users who comply with this policy. The processed dataset and the association map are sent to a private cloud for geometric perturbation (Fig. 1).

C. Geometric Perturbation

The field or column names to be managed are collected for each mapping in the association map. A random geometric disturbance key is generated, which is a multiplication transformation sequence (TP), a translation (Vs) and a distance disturbance (D).

$$GDP(P) = TP + V_S + D$$

Where D is given as

$$D = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{(x-\mu)^2}{2\sigma^2}}$$

TABLE I. Dataset and its Classes

Class 1	Overly sensitive information that cannot be shared by the data owner
Class 2	Sensitive information that can be shared and fine grain controlled for the accessing users.
Class 3	Insensitive information that can be shared without any security concerns

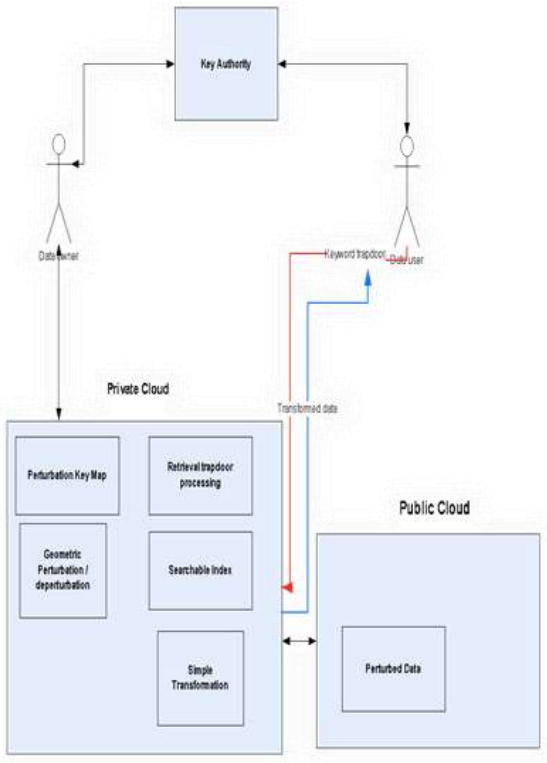

Fig. 1. Architecture of SFAC-SHC.

Where T is a random projection matrix, P is a matrix to be transformed, Vs is a translation matrix, D is a random Gaussian noise. The advantage in this disturbance is that even after the perturbation has been applied, geometric properties such as distance are preserved in the transformed dataset. The fields in the data to be tested are copied to a separate table along with the corresponding identifier. Leaving the identifier, the rest of the columns in the separate table are disturbed by using the generated geometric disturbance key. For this disturbed data, a random file name is created, and this file is transferred to the public cloud for storage. An entry is added to the perturbation key map mapping between the hash of the private key and the following information:

Hash (Private key)	Field name perturbed Perturbation key Perturbed file name (saved in a public cloud) Private key

The hashing function to be used is transmitted to the private cloud by the data owner. The data owner also sends this hashing function to the main authority to distribute it to the data users. Data Perturbation algorithm is used for geometric disturbance.

D. Data Perturbation Algorithm

Input: Original data D, its size n *and delicate characteristic* $[S]$

output: Perturbed data set D^I

Steps:

a) The sensitive attributes are rotated 180° clockwise and the result is a rotation matrix $[RT]_{n\times1}$

b) The result of $[RT]_{n\times1}$ and the $[S]_{n\times1}$ is obtained in step 3. The duplicated esteems will be, $[X]_{n\times1}=[RT]_{n\times1}\times[S]_{n\times1}$

c) The translation transformation matrix is computed $[T]$ as a mean of sensitive attribute $[S]_{n\times1}$

d) Generate transformation $[TS]_{n\times1}$ by applying the transformation matrices to $[S]_{n\times1}$.

e) Compute Gaussian distribution as a probability density function for Gaussian noise $\Omega=\frac{1}{\sigma\sqrt{2\pi}}e^{\frac{(x-\mu)^2}{2\sigma^2}}$

where μ = mean and σ = variance

f) Now the perturbation data is $D^I=[X]_{n\times1}+[VS]_{n\times1}+\Omega$

It is detailed in our earlier work [20].

In addition to perturbation, a searchable index is constructed between the field values to the row index of the dataset.

E. Secure Retrieval

The data user can retrieve data in two modes-all data or fit a specific field value pair.

For retrieval in all data mode, the data user first retrieves the private key from the key authority for its corresponding attributes. The private key and the hashing function are returned to the key authority. The secret key is hacked and then sent to the private cloud. At the private cloud, a lookup is performed on a disturbance key mapping to find a match for a hashed private key. If a match could not be identified, the retrieval would fail. If a match is found, the following information is retrieved from the mapping:

1) Field name perturbed
2) Perturbation key
3) Perturbed file name (saved in a public cloud)
4) Private key.

The disrupted file is retrieved from the public cloud, and the de-disruption key is retrieved from the files. We use the Data De-disruption algorithm given below for geometric de-disruption.

F. Data De - Perturbation Algorithm

Input: Perturbed data D^I, sensitive attribute $[S]$

Output: Original data D of the perturbed data D^I

Steps:

a) Given the perturbed dataset D^I, its tuple estimate n and the relating sensitive attribute $[S]_{n\times1}$

b) Sensitive attribute $[S]_{n\times1}$ is rotated in 180° counter clock-wise direction, so the random rotation matrix $|RT|_{n\times1}$ is is generated.

c) The result of $[RT]_{n\times1}$ is and $[S]_{n\times1}$ is obtained in step 3. The duplicated esteems will be, $[X^I]_{n\times1}=[RT]_{n\times1}\times[S]_{n\times1}$

d) Compute the translation transformation matrix $[TS]_{n\times1}$ as mean of sensitive attribute $[S]_{n\times1}$

e) Generate transformation $[VS^I]_{n\times1}$ by applying the transformation matrices to $[S]_{n\times1}$

f) Compute Gaussian distribution Ω^I

g) Now the result data is $P=[X^I]_{n\times1}+[VS^I]_{n\times1}+\Omega$

The data after de-disruption must not be submitted directly to the customer. The private key, along with the current hour, is hashed to a numeric code and a simple transformation operation is performed on the values of the field with a numeric code (like a progressive addition). This transition helps prevent attacks from being captured by the network. At the end of the data user, the opposite of simple transformation (like progressive subtraction) is performed using the private key and the current time to get the original data.

The retrieval method is secure against network capture attacks due to the exchange of only transformed data between the private cloud and the user. The data retrieval from cloud to user end is masked with a quick transformation. Without the details on the private key and the parameter used for hashing (here is the current time), the removal of the mask is not possible. Even if a network capture attack is performed, the recovered data is still masked and stable.

The proposed scheme also supports the importance of the field retrieval. The field and the corresponding value to be searched are encrypted by a private key using an asymmetric cryptographic algorithm and sent to a private cloud. This encrypted value is called a search door. Because the field name and corresponding value are encrypted, it is difficult for the network to catch attacks to compare between the search information and the outcome. The filed name and the corresponding meaning are decrypted in the private cloud. Lookup is performed on a disturbance key mapping to find the match. If a match could not be identified, the retrieval would fail. If a match is made, the following information is recovered from the mapping table:

1) Field name perturbed
2) Perturbation key
3) Perturbed file name (saved in the public cloud)
4) Private key.

If the field name given for the search in the field name list has been interrupted, the search will continue, otherwise the error will be returned. The fine-grained access control is then applied even while searching. The value of the search field is searched in the searchable index of the match field. If no matching row index is found, an error is returned. If indexes of the matching row are found, those specific row indexes will be retrieved from the public cloud. De-disruption occurs in the obtained row indexes. If the field name given for the search in the field name list has been interrupted, the search will continue, otherwise the error will be returned. The fine-grained access control is then applied even while searching. The value of the search field is searched in the searchable index of the match field. If no matching row index is found, an error is returned. If indexes of the matching row are found, those specific row indexes will be retrieved from the public cloud. De-disruption occurs in the obtained row indexes. The data after de-disruption must not be submitted directly to the customer. The private key, along with the current hour, is hashed to a numeric code and a simple transformation operation is performed on the values of the field with a numeric code (like a progressive addition). At the end of the data user, the opposite of simple transformation (like progressive subtraction) is performed using the private key and the current time to get the original data.

IV. Proposed Solution

The proposed solution has the following novel aspects:

1) The data owner has more control over highly confidential information and though the data is uploaded to the cloud. This is activated by transferring unnecessarily confidential information to Class 1 and encrypting the data owner's public key. This information cannot be accessed without the owner sharing this key.

2) The data transmitted from the cloud to the user is simply translated to the private key and the current time. It is also difficult for network attackers to collect and decode information from it.

3) Users accept two types of retrieval. Retrieval may be either a whole file or several records that meet a criterion.

4) Fine-grained field-level access control is implemented for users in both retrieval modes.

5) The data owner has more control about which users he wants to share data based on the user's attributes.

V. Results

The performance of the proposed searchable fine access control on secure hybrid clouds (SFAC-SHC) is compared in different aspects of

- Perturbation efficiency.
- Data storage and retrieval efficiency.
- Security against attacks.

The arrhythmia dataset from the UCI machine learning repository is used for evaluation [21].

A. Perturbation Efficiency

The disturbance efficiency of the proposed solution is compared to the RG+RP algorithm proposed in [12]. K-Means clustering is done on the original data as well as on the disrupted data produced by the proposed RG+RP. The accuracy of the clustering is determined between.

1) The clusters used the proposed cluster and the initial data set cluster.

2) Clusters used RG+RP and the cluster of the original data set.

The clustering accuracy is calculated as

$$ACC = \frac{1}{N}\sum_{i=1}^{k}\left(\left|Cluster_i\left(P\right)\right| - \left|Cluster_i\left(P^I\right)\right|\right)$$

Where P is the original data, P^I is the transformed data, k is the number of clusters and N is the number of items in the dataset. The result of clustering accuracy (Table II) is measured for different k values and the result.

The clustering accuracy (Fig. 2) lies more in the proposed solution as the transformation method adopted retains the geometrical properties even after transformation.

TABLE II. RESULT OF CLUSTERING ACCURACY FOR DIFFERENT VALUES OF K

K	Clustering accuracy in RG+RP [12]	Clustering accuracy in Proposed
2	66.23	65.89
3	66.56	71.25
4	73.33	74.59
5	67.22	79.58

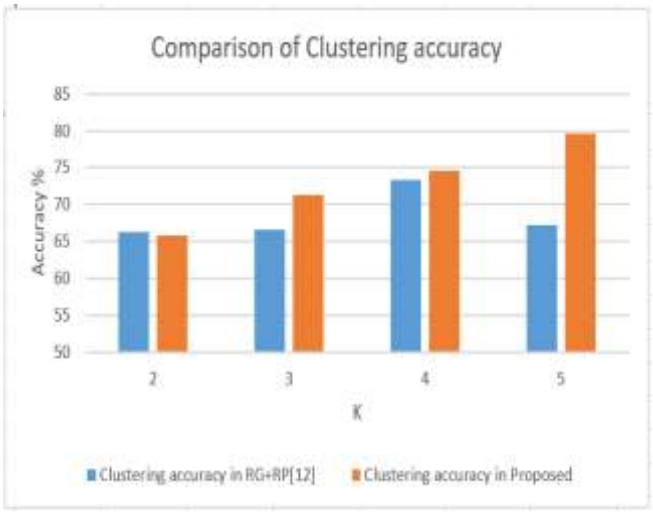

Fig. 2. Comparison of Clustering Accuracy.

B. Data Storage and Retrieval Efficiency

Performance of the proposed method is compared with a similar approach to the fine-grained searchable retrieval system proposed in [5]. Output is contrasted with the following parameters by changing the number of attributes:

1) Key generation time.
2) Index generation time.
3) Trapdoor generation time.
4) Search time.

The key generation time (Fig. 3) is comparatively shorter in the proposed solution as the key size (16 bytes) is shorter in the proposed solution compared to [5].

The index generation time (Fig. 4) is shorter in the proposed solution compared to [5] as the index is computed only in certain fields as needed by users. But the index [5] is optimized for all fields, and this increases the generation time of the index.

The time of generation of trapdoor (Fig. 5) or encrypted search keywords in the proposed solution is lower than [5]. This reduction is due to the reduced key size and the less rounded AES for trapdoor generation in the proposed solution.

Retrieval time (Fig. 6) is also shorter in the proposed solution compared to [5]. Reasons for shorter recovery time are attributed to lower rate of trapdoor decryption, index scanning, and lower time for de-disruption and easy transformation.

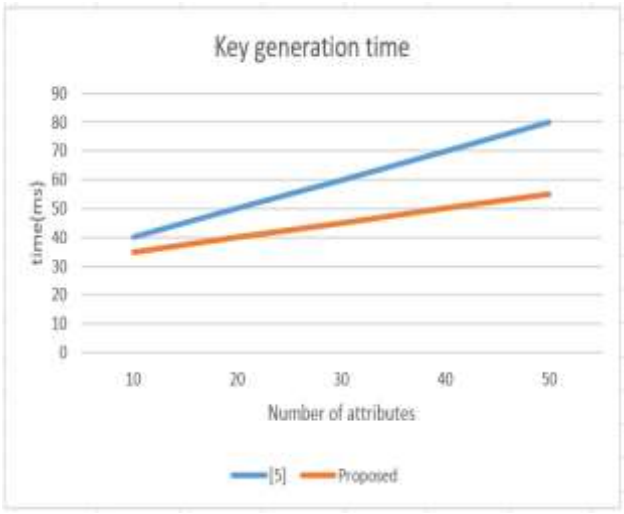

Fig. 3. Key Generation Time.

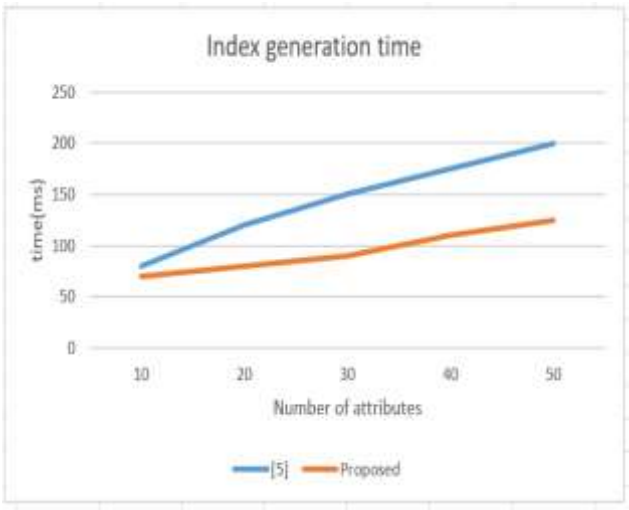

Fig. 4. Index Generation Time.

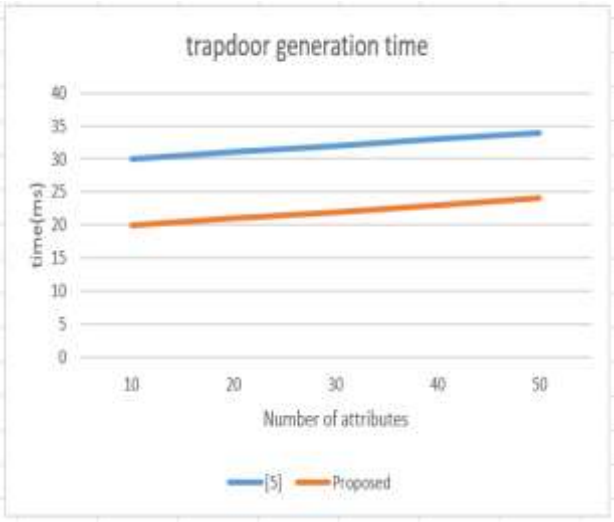

Fig. 5. Trapdoor Generation Time.

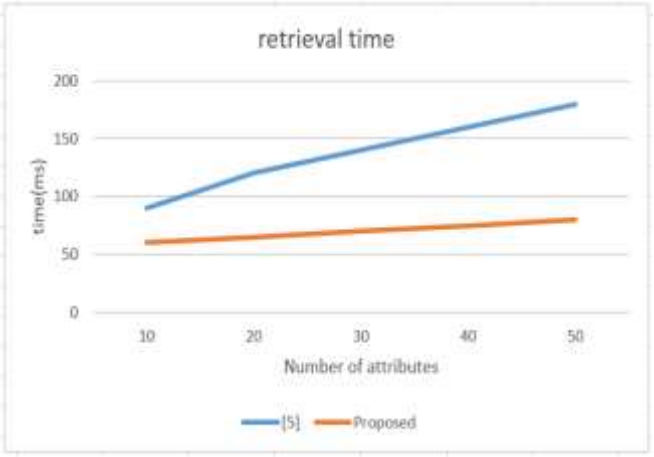

Fig. 6. Retrieval Time.

Fig. 7. VOD Overtime.

C. Security against Attacks

The security of the proposed solution is measured in terms of the complexity of estimating the original data from the disrupted data by an intruder who extracts the disrupted data from the cloud. There are two types of fields to protect privacy in the dataset:

1) Class 1
2) Class 2

Class 1 data is overly sensitive. Class 2 is confidential information that can be shared, and fine grain regulated for users who have access to it. In the proposed scheme, the Class 1 fields are encrypted with AES and geometric disturbances are added if they need to be exchanged. Class 2 fields are subject only to geometric disturbance. The variance of the difference-based method is used to measure the degree of difficulty. Let the difference between the data in the original column and the projected data be the random variable Di. Without any knowledge of the original results, there is a mean and variance of the difference in the accuracy of the calculation. Since the mean difference can be easily omitted if the attacker can approximate the original column distribution, only the difference variance (VoD) is used as the primary metric to evaluate the degree of difficulty in estimating the original results.

Let X_i be a random variable representing the column i, X_i^I be the estimated result of X_i and difference $D_i = X^i - X$ Let mean of D be $E(D_i)$ and variance is $Var(D_i)$. VOD for column i is $Var(D_i)$. VOD is measured for each column and average VOD is given as a privacy measure(pm)

$$pm = \frac{\sum_{i=1}^{N} VOD_i}{N}$$

A guess is launched for 5 hours on the perturbed data and the privacy measure (pm) is measured for every 1-hour interval and plotted below.

It can be seen from the results that VOD (Fig. 7) in the proposed solution is extremely high compared to VOD in [5]. Higher VOD means that it is difficult to locate the closest approximation of the original data from the disturbed data. VOD increased in the proposed solution due to geometric disruption combined with encryption for data fields of class 1.

VI. Conclusion

In this work, a searchable fine access control for stable hybrid clouds (SFAC-SHC) is proposed. The scheme uses multiple concepts of CP-ABE, fine-grained access control, geometric disruption, and searchable indexing of disrupted data. Stable Perturbed data is maintained in an untrusted public cloud with no chance of leakage. The information needed to interrupt data on the public cloud is stored in the private cloud. The proposed scheme is safe against network capture attacks and unauthorized access attacks. Fine-grained access control is a field-wise exercise, so that knowledge is strictly regulated. The work is focused on the premise that there is full confidence in the private cloud. As future work, the work needs to be optimized for a semi-trusted private cloud by unloading some of the operations to the respective data owner or data consumers.

References

[1] X. Liu, R.H. Deng, Y. Yang, H.N. Tran, and S.Zhong, Hybrid privacy-preserving clinical decision support system in fog–cloud computing, Future Generation Computer Systems.2018; vol.78,pp.825-837.

[2] Zhang, Xuyun, et al. "Proximity-aware local-recoding anonymization with mapreduce for scalable big data privacy preservation in cloud." IEEE transactions on computers 64.8 (2014): 2293-2307.

[3] Li, Jin, et al. "Secure attribute-based data sharing for resource-limited users in cloud computing." Computers & Security 72 (2018): 1-12.

[4] Achampong, Emmanuel & Dzidonu, Clement. (2016). Optimising Attribute-based Encryption to Secure Electronic Health Records System within a Cloud Computing Environment. 27-34. 10.21742/ijcs.2016.3.2.04.

[5] Jin Sun, Xiaojing Wang, "A searchable personal health records framework with fine-grained access control in cloud-fog computing",PLOS ONE,2018.

[6] J. Yang, J. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment", Future Generation Computer Systems, Vol. 43-44, No. 2, pp. 7486, 2015.

[7] Kao, Yuan-Hung & Lee, Wei-Bin & Hsu, Tien-Yu & Lin, Chen-Yi & Tsai, Hui-Fang & Chen, Tung-Shou. (2015). Data Perturbation Method Based on Contrast Mapping for Reversible Privacy-preserving Data Mining. Journal of Medical and Biological Engineering. 35. 10.1007/s40846-015-0088-6.

[8] Yun, Unil & Kim, Jiwon. (2015). A fast perturbation algorithm using tree structure for privacy preserving utility mining. Expert Systems with Applications. 42. 1149–1165. 10.1016/j.eswa.2014.08.037.

[9] J.Li, J.Li, X.Chen, Z.Liu, and C.Jia, Privacy preserving data utilization in hybrid clouds, Future Generation Computer Systems.2014;vol.30, pp.98-106.

[10] H. Zhang, Z. Zhou, L. Ye and X. Du, "Towards Privacy Preserving Publishing of Set-Valued Data on Hybrid Cloud," in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 316-329, 1 April-June 2018.

[11] Z. Zhou, H. Zhang, X. Du, P. Li and X. Yu. Prometheus: Privacy-Aware Data Retrieval on Hybrid Clouds. In Proc. of INFOCOM, 2013.

[12] Lyu, Lingjuan & Bezdek, James & Law, Yee Wei & He, Xuanli & Palaniswami, Marimuthu. (2018). Privacy-preserving collaborative fuzzy clustering. Data & Knowledge Engineering. 10.1016/j.datak.2018.05.002.

[13] Chen, Keke & Sun, Gordon & Liu, Ling. (2007). Towards Attack-Resilient Geometric Data Perturbation. 10.1137/1.9781611972771.8.

[14] Chen, K., Liu, L. Geometric data perturbation for privacy preserving outsourced data mining. Knowl Inf Syst 29, 657–695 (2011).

[15] X. Yuan, X. Wang, C. Wang, J. Weng and K. Ren, "Enabling Secure and Fast Indexing for Privacy-Assured Healthcare Monitoring via Compressive Sensing," in IEEE Transactions on Multimedia, vol. 18, no. 10, pp. 2002-2014, Oct. 2016.

[16] A. Majeed, "Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data," Journal of King Saud University - Computer and Information Sciences, 2018.

[17] Li, Jiuyong & Liu, Jixue & Baig, Muzammil & Wong, Raymond. (2011). Information based data anonymization for classification utility. Data Knowledge. Eng. 70. 1030-1045. 10.1016/j.datak.2011.07.001.

[18] P. Cheng, J. Roddick, S. Chu, and C. Lin, "Privacy preservation through a greedy, distortion-based rule-hiding method," Applied Intelligence, vol. 44, no. 2, 2015, pp. 295-306.

[19] Sabin Begum, R., Sugumar, R. Novel entropy-based approach for cost-effective privacy preservation of intermediate datasets in cloud. Cluster Comput 22, 9581–9588 (2019).

[20] Vulapula Sridhar Reddy,Barige Thirumala Rao,"A Combined Clustering and Geometric Data Perturbation Approach for Enriching Privacy Preservation of Healthcare Data in Hybrid Clouds",International journal of engineering and systems,Oct 2017.

[21] https://archive.ics.uci.edu/ml/datasets/Arrhythmia.

[22] Ruth Ramya K., Saikrishna D.N.V., Sravya Nandini T., Tanmai Gayatri R," A survey on using biometrics for cloud security".International Journal of Engineering and Technology(UAE),2018.

[23] Vurukonda N., Thirumala Rao B.,"Hash counter hash method for privacy and security in cloud computing with attribute-based encryption",Journal of Advanced Research in Dynamical and Control Systems,2017.

[24] Ranjeeth Kumar M., Srinivasu N., Reddy L.C.,"Fine grained multi access control via group sharing in distributed cloud data",Journal of Theoretical and Applied Information Technology,2017.

[25] Wadhya R., Divya Harika B., Sandeep Reddy C., Krishna Reddy V.,"Security for data storage in cloud",Journal of Advanced Research in Dynamical and Control Systems,2017.

[26] Vurukonda N., Thirumala Rao B.,"Secure sharing of outsourced data in cloud computing with comparison of different attribute based encryption",Journal of Advanced Research in Dynamical and Control Systems,2017.

[27] Dr.V.Naresh, T.Gopi Venkata Ajay, T.Naga Sai Reddy, M.Srinivas,"An Efficient And Privacy Preserving Biometric Authentication Scheme In Cloud Computing", International Journal Of Scientific & Technology Research Volume 9, Issue 01, January 2020 Issn 2277-8616.

[28] Vulapula Sridhar Reddy, Malladi Srinivas," Secure Data Accessing Over Cloud Computing Environment Using Hybrid Query", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 14-Special Issue, 2018.