Fuzzy-Set Based Privacy Preserving Access Control Techniques in Cloud (FB-PPAC)

Sushmita Kumari, Sudha. S, Brindha. K
School of Information Technology and Engineering, VIT University, Vellore - 632014, Tamil Nadu, India

Article Info

Article history:

Received Aug 17, 2017
Revised Oct 19, 2017
Accepted Nov 2, 2017

Keyword:

Blinded RSA
Encryption
Fuzzy set theory

ABSTRACT

The word “Cloud” refers to network or internet. It is present at.remote location. Cloud computing is a latest mechanism used now-a-days for accessing, manipulating and configuring applications online via internet. It allows users for online data storage, various applications and infrastructure. There are few downsides of cloud computing like in public cloud sharing of data, selected data shared with users of various level without confidentiality and privacy of data. Different methods were used to fix this problem like encryption of attribute; encryption of access control but they have their own problems related to big computation for accquiring access structure, invoking and behavior management. So for removing these weakness, the combination of fuzzy-set theory and RSA algorithm has been introduced. Fuzzy-set is used for clustering the data based on their points. Further for privacy, I have included RSA for encryption and decryption of data which is used to store in cloud database. The analysis of my experiment shows the system is efficient, flexible and provides confidentiality of the data.

Corresponding Author:

Sudha.S,
School of Information Technology and Engineering,
VIT University,
Vellore - 632014, Tamil Nadu, India.
Email: sudha.s@vit.ac.in

1. INTRODUCTION

The cloud computing is a developing innovation which is quickly picking up notoriety as a different option for conventional data innovation. Cloud computing conveys a more adaptable environment for colossal measures of information that are utilized as a part of different applications and administrations through on-interest self-administrations. One essential trademark towards this outlook changing is that information are being combined and outsourced into clouds. The cloud outsourced capacity administrations bear the cost of another benefit development for the client by method for offering an area free stage, adaptability support for dealing with their information. The cloud storage service (CSS) discharges the weight of information stockpiling administration and support. Despite the fact that, if this administration vulnerable to any assaults or disappointments, it would convey extreme monetary misfortunes to clients as their information are put away into an untrusted pool of capacity outside the client undertakings. These sorts of security dangers forced because of taking after reasons: the cloud computing frameworks are a great deal more solid and intense than client individualized computing gadgets. Nonetheless, they are still helpless against different security dangers both from inside and outside the cloud clients for the advantages of their ownership. In this way, it is essential for cloud service suppliers to offer high privacy to the information that is added on it. In this way, we need a suitable access control strategies to secure the information access in the cloud. The traditional access control systems that are utilized as a part of unchangeable appropriated environment can be categorized as Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role based Access Controls (RBAC).

DAC is utilized in circumstances that receive each article has a proprietor that could control the access rights to the item. MAC expect that system admin has the control to make the strategies and subjects or proprietors don't have the ability to override the approach. RBAC is the model which gives the client access based on the role of the clients. In every one of these models clients and assets are recognized by the different names. These models are not fitting for the dynamic distributed environment, for example, grid and cloud computing where clients are distinguished by their qualities and not by predefined personalities. By seeing all these problem I have proposed fuzzy set based access control technique.

The main aim of this project is to apply fuzzy set theory for privacy preserving in cloud. So a web application on job portal is created. In which Fuzzy C Mean Clustering algorithm is used for displaying the status of each applicant for the job they have applied. In this application RSA algorithm is also used for encryption purpose. The entire data will be stored in cloud server. Microsoft Azure account and visual studio is used for this project.

The proposed system in [1] is based on Hierarchy Based Privacy Preserving Access Control technique in public clouds. It utilizes the blinded encryption and decryption procedure, for a secured access control technique in cloud. The users are divided into various roles and where provided with security key once they provide their identity to the trusted authority. When the data owner wants to upload the file the blinded part of file is uploaded and encrypted in cloud. When the user request to access a file, then the encrypted file, encrypted secret key and session key is decrypted and returned to the user except the blinded part. Then user ask TA for unblind value for decryption and user remove the blind part and view the data. This process reduces the time complexity into some extent.

The proposed method ABE in [5], [7], [13, 14], RBAC in [4, 5], [10] and ABAC [6], [8] are some of the techniques which are utilized for outsourced data in cloud. ABE stands for Attribute Based Encryption was discovered by sahai and waters [2] to use in implement access control techniques taking into account different properties. The two variety of ABE like CP-ABE [2] and KP-ABE [6] was introduced by Goyal and Bethencourt et al. Yet, utilizing this technique straight forwardly, to an association was not fitting which organized with progressive level of clients.

Yu et al. [8] recommended a plan to perform secure, fine grained and versatile access control in cloud computing. It embraces KP-ABE with a re-encryption strategy for supporting effective client denial. With KP-ABE plan, the information proprietor can't have control that who can unscramble the content. Wan et al. [15] recommended a plan to accomplish versatile and fine grained access control for the clients who works in various level association structure. They develop the current CP-ABE plan with the various leveled client structure. This plan needs in general framework adaptability as it makes the information customer to perform the decoding. Wang et al [3] offered a plan by consolidating CP-ABE with hierarchical Identity-based encryption (HIBE) to achieve fine grained and versatile access control with the progressive client structure. This plan does not bolster compound qualities and numerous worth task to traits. Sushmita Ruj et al [13] recommended a distributed access control plan for information access in cloud environment. It utilizes both Attribute Based Encryption and Attribute Based Signature plans to give effective client denial and mysterious validation. It utilizes the case approach to avert replay assaults in cloud outsourced information.

A few RBAC variety model [4, 5] is introduced to suite the disseminated environment needs that is expected to fulfil the large scale industry. The paper [5] brought up this problem and proposed a part and association based access control model to conquer this issue. In the existing system [4] distributed Role Based Access control model is introduced for overcoming the extensible issues. Despite the fact that, these model shows change as far as execution proficiency and adaptability, the techniques neglected to give broad answer for versatility issue. Notwithstanding this, the RBAC display still endure by part blast issue [10] which is confronted by a few substantial scale venture that requires fine grain access control than what the current RBAC underpins.

The existing system [6] utilizes the Two-Layer Encryption approach, in which the arrangements are divided into two sections. The information proprietor that conveys the primary piece of ACP approaches performs the inward layer encryption. The external layer encryption performed by the cloud administration suppliers as per the second part of ACP's. However, none of these ABAC based plans recommended an answer to cluster the clients as per the distinctive prerequisites of big business polices so client seeking should be possible productively. As of late, a few scientists centered for giving fine grained access control answer for mobile cloud computing environment.

Mohan et al [11] introduced an access control plan in cloud environment taking into account polynomial based methodology. The information proprietor utilizes the polynomial based mystery sharing plan for key sharing and uses symmetric encryption procedure for information encryption. In any case, no trial investigation included for contrasting the execution of this plan and ordinary marks plans. By considering every one of these elements in different plans, the fuzzy set based security safeguarding access control strategies are proposed to give the answer for gathering the clients and validation based on group signature [16] and further give the answer for backing effective use of storage room and backing for element client expansion [17].

2. RESEARCH METHOD

Clustering means combining set of objects such that object of similar type are in one group and dissimilar in other group. Fuzzy clustering information components can fit in with more than one cluster, and connected with every component is an arrangement of participation levels. These demonstrate the quality of the relationship between that information component and a specific cluster. Fuzzy clustering is a procedure of appointing these participation levels, and after that utilizing them to dole out information components to one or more clusters. Clustering is of different types and can be used in various area. I have used Fuzzy C-Means clustering method. Shown in Figure 1 System Architecture.

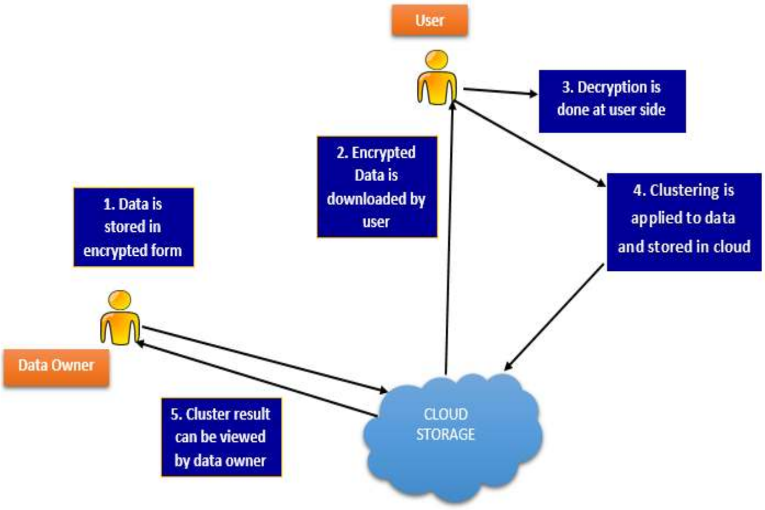
User
3. Decryption is done at user side
2. Encrypted Data is downloaded by user
4. Clustering is applied to data and stored in cloud
1. Data is stored in encrypted form
Data Owner
5. Cluster result can be viewed by data owner
CLOUD STORAGE

Figure 1. System Architecture

2.1. Grouping based on data provided

The data is grouped based on their functionality and other characteristics like in our system grouping of job is done based on functional area, year of experience, location. The Boolean function is used for AND (Ʌ) and OR (V) is used. For example (m1Ʌm2Ʌm3), (m1)V(m2Ʌm3), (m1Ʌm2)V(m3), (m1Vm2Vm3), (m1Ʌm3)V(m2) where m1,m2 and m3 are attributes.

2.2. Encryption

The steps included in encryption process are:-

1. Generate a Rijndael Managed asymmetric key for encrypting the data.
2. When the encryption is done using Rijndael key then the RSACryptoservice object is created to encrypt the Rijndael key.
3. Then cryptostream object is used to read and encrypt the source file in blocks of bytes in destination file object.
4. The byte array is created by finding the length of encrypted key and IV.
5. The key size, IV and their length is written to encrypted package.

The general method for encryption and decryption include generating the private key and public key using the given method:

a) Select two prime number X and Y
b) Find M=X*Y and ϕ(M)=(X-1)*(Y-1)
c) Select p such that 1<p< ϕ (M) and p and M are coprime
d) Find the vaue for z such that (z*p)% ϕ (M)=1
e) Now Public Key is (p,M) and Private key is (z,M)

f) Encryption is q≡c^{p}(mod)M

2.3. Decryption

The steps included in decryption process are:-

1. Generate a Rijndael Managed asymmetric key for decrypting the data.
2. Then in byte array obtain the length IV, encrypted key and the first eight bytes of file.
3. Now RSA object is created to decrypt the Rijndael Managed key.
4. Then cryptostream object is used to decrypt the cipher text of file in blocks of bytes.
5. Decryption is c≡q^{z}(mod)M

The RSA Key size 256 is used, IV length is between 4-7 bytes. The RSA algorithm can’t encrypt the larger file so for that purpose the data is encrypted using asymmetric key and then the asymmetric key is encrypted using RSA.

2.4. Clustering

The Fuzzy-C Mean clustering is used. The FCM clustering formula used here is $Q_m = \sum_{i=1}^{K} \sum_{j=1}^{C} v_{ij}^{n} \left\| Z_i - Y_j \right\|^{2}$ 1≤n<∞

where n is a real number, v_{ij} is the degree of association of z_i in the cluster j, z_i is the ith of d-dimensional measured data, y$_j$ is the d-dimension centre of the cluster, and ‖*‖ is a standard communicating the likeness between any deliberate information and the centre. $\left\| Z_i - Y_j \right\|$ is the Euclidean distance between z_i and y$_j$. The fuzzy partition is carried out through iterative function by updating the value of v_{ij} *and* Y_j *as follows:*

$$v_{ij} = \frac{1}{\sum_{k=1}^{C} \left(\left\| \frac{Z_{i-} Y_j}{Z_{i-} Y_k} \right\| \right)^{\frac{2}{m-1}}}$$

$$Y_j = \frac{\sum_{i=1}^{N} v_{ij}^{m} Z_i}{\sum_{i=1}^{N} v_{ij}^{m}}$$

2.4. Case Study

Shown in Figure 2 Job Portal Hierarchy. A web application on Job Portal named Career Finder is created. The application is designed in Visual Studio using net language. There are three entities in this application they are:

a) Admin: - The purpose of admin is to just view, edit or delete the job seeker and job provider details.

b) Job Seeker: - First the job seeker has to register in the portal and provide all the necessary detail asked in portal. After that when the seeker login the portal there will be three option available for seeker edit detail, check available jobs and home screen. In check available jobs page the grouping function is used based on this formula (m1Λm2Λm3), (m1)V(m2Λm3), (m1Λm2)V(m3), (m1Vm2Vm3), (m1Λm3)V(m2) where seeker function is (m1), total year of experiences is (m2) and location is (m3). The seeker can check job and apply for it. Before applying the seeker first have to select the job and select the resume which will be encrypted and then stored in cloud. Then there is track application page where seeker can see there job status whether they are qualified, overquailifed or underqualified.

c) Job Provider: - The job provider can view or add new jobs, check and update score for each applicant, check final result and edit their own details. In check and update score for each applicant the provider has to first download the encrypted resume from the database which is created in cloud. After downloading the encrypted resume there is another option available to decrypt the encrypted resume from there the resume will be decrytpted and stored in user system. After decryption is done the provider have to insert the technical score and hr score then partial FCM clustering is performed using this score. In result page the other halves of FCM clustering is performed and the result is displayed based on the clustering.

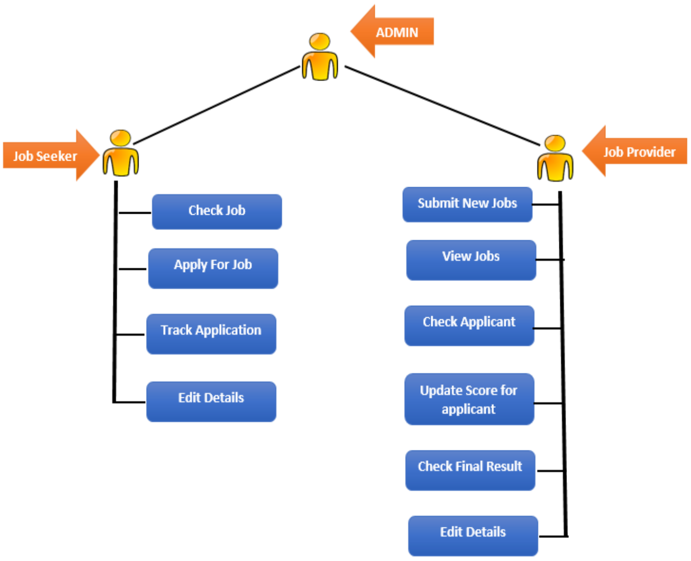

Figure 2. Job Portal Hierarchy

3. RESULTS AND ANALYSIS

The experiment was done on a laptop with 3.10 GHZ CPU and 4GB RAM, running windows 10 as well as tested in windows 7 OS. The performance was checked and found better than the existing system. The data which is stored in cloud was taken from internet.

The chart has been prepared to show the difference between time taken by existing system and proposed system for encryption, decryption and data transmission. Shown in Table 1-2, and Figure 3-4.

Table 1. Average File Upload of both existing and proposed system

File size	27KB	52KB	172KB	520KB
HB-PPAC [1] (Time in ms)	32.71	37.58	48.25	55.53
FB-PPAC (Time in ms)	28.53	32.42	43.31	49.2

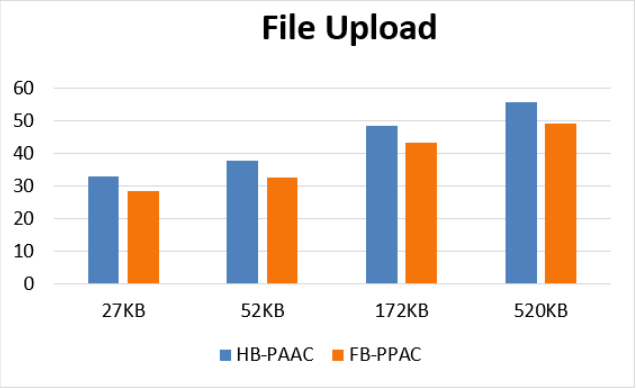

Figure 3. Average File Upload of both existing and proposed system

Table 2. Average File Download of both existing and proposed system

File size	27KB	52KB	172KB	520KB
HB-PPAC [1] (Time in ms)	23.68	26.51	34.89	42.19
FB-PPAC (Time in ms)	20.53	21.42	29.31	38.2

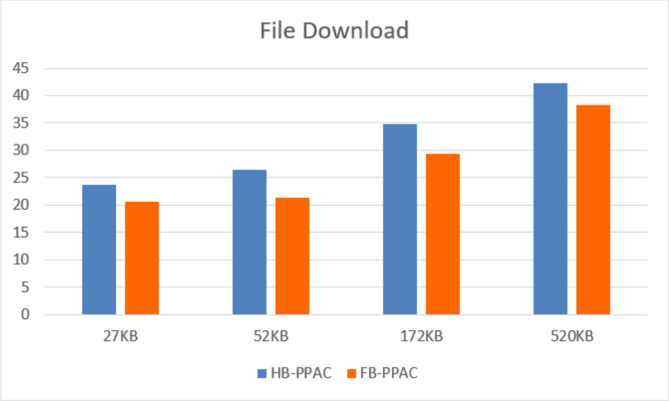

Figure 4. Average File Download of both existing and proposed system

The encryption and decryption time varies according to the file size. Hence the result shows the proposed system is more reliable and fast then exisiting system.

4. CONCLUSION

In this paper, fuzzy set based privacy preserving access control technique is used to provide privacy for accessing public data in clouds. The fuzzy c-mean clustering is used for clustering the data by user side. The encryption is done at data owner side for encrypting the data and stored in cloud database. The decrption is done at user side for decrypting the data. By using this method it makes the system unique from other existing system. The experimental analysis proves that system performs better by minimizing the computation cost and increase the performance speed.

ACKNOWLEDGEMENTS

Aside from the endeavors made by me, the achievement of the task depends generally on the support and guidelines of many others. We would take this chance to express our appreciation to the people who have been instrumental in the fruitful completion of this project.

REFERENCES

[1] Sudha Senthilkumar, Madhu Viswanatham, (in press). HB-PPAC: hierarchy based privacy preserving access control technique in public clouds, *International Journal of High Performance Computing and Networking.*

[2] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." *Security and Privacy, 2007. SP'07.IEEE Symposium on*. IEEE, 2007.(6)

[3] Cadenhead, Tyrone, Murat Kantarcioglu, and Bhavani Thuraisingham. “Scalable and efficient reasoning for enforcing role-based access control.” *Data and Applications Security and Privacy XXIV*. *Springer Berlin Heidelberg*, 2010. 209-224.

[4] Elliott, Aaron, and Scott Knight. “Role Explosion: Acknowledging the Problem.” In *Software Engineering Research and Practice*, pp. 349-355. 2010.(10)

[5] Freudenthal, Eric, et al. "dRBAC: distributed role-based access control for dynamic coalition environments." *Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on*. IEEE, 2002.(9)

[6] Fan, Bin, et al. "Cuckoo Filter: Practically Better Than Bloom." *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*.ACM, 2014.(14)

[7] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data" *Proceedings of the 13th ACM conference on Computer and communications security*.Acm, 2006.(5)

[8] Grobauer, B., Walloschek, T. and Stocker, E. (2011) “Understanding cloud computing vulnerabilities.” *IEEE Security and Privacy*, Vol. 9, pp.50–57.(23)

[9] Li, Qi, Mingwei Xu, and Xinwen Zhang "Towards a group-based RBAC model and decentralized user-role administration." *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on.* IEEE, 2008.(2)

[10] Mohan, and M. Sudheep Elayidom. "Fine Grained Access Control and Revocation for Secure Cloud Environment–A Polynomial Based Approach." *Procedia Computer Science* 46 (2015): 719-724.(17)

[11] Ruj, Sushmita, Milica Stojmenovic, and Amiya Nayak. "Decentralized access control with anonymous authentication of data stored in clouds." *Parallel and Distributed Systems, IEEE Transactions on* 25.2 (2014): 384-394.(15)

[12] Su, Jin-Shu, et al. "Attribute based encryption schemes." *Journal of Software* 22.6 (2011):1299-1315.(1)

[13] Wan, Zhiguo, Jun E. Liu, and Robert H. Deng."HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *"Information Forensics and Security, IEEE Transactions on* 7.2 (2012): 743-754.(7)

[14] Yang, Piyi, Zhenfu Cao, and Xiaolei Dong. "Fuzzy Identity Based Signature."*IACR Cryptology ePrint Archive* 2008 (2008): 2.

[15] Senthilkumar, S., and Viswanatham, M. *ACAFD:* Secure and Scalable Access Control with Assured File Deletion for Outsourced Data in Cloud. *Journal of ICT Research and Applications, (2014) 8(1), 18-30.*

[16] Carlin, Sean; Curran, Kevin. Cloud Computing Technologies. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.1, No.2, June 2012, ISSN: 2089-3337.

[17] Kumar, Ashish. World of Cloud Computing & Security. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.1, No.2, June 2012, ISSN: 2089-3337.