Real Time Class Based Encryption for Efficient Data Security in Cloud Environment using User Profile

Kumaresan S, Vijayaragavan Shanmugam

Abstract: ***The data security in cloud has been well studied towards the data present in the cloud environment. Number of techniques has been discussed earlier and each produces different performance results in data security. But still there are gaps in performance in security which should be optimized. To improve the security performance, an efficient class based encryption (CBE) with User profile (UP) is presented. The proposed CBE-UP method groups the cloud data at attribute level based on the importance mentioned in the taxonomy. The data taxonomy covers various information related to the attribute of any data point like their sensitivity, importance in different class and so on. According to the taxonomy, the method estimates the Class Sensitivity Measure (CSM) for each attribute, which has been used to classify the data attribute. Further, for each Attribute class, the method generates different key from the key set and assigns various scheme to perform encryption and decryption. The selection of key and method has been iterated at each time window. The performance of data security has been improved and reduces the network overhead in distribution of keys to the registered users.***

Index Terms:
Cloud Security, CBE, User Profile, Cloud Environment, Data Security, CSM.

I. INTRODUCTION

The increasing size of organizational data challenges the administrators in maintaining their data in centralized servers or their own servers. Also, the most organizations have not enough funds to purchase high configuration computers and data servers. This encourages the organizations moving towards the cloud environment in maintaining their data. There are organizations which provide cloud services to support access and maintenance of data in cloud. The Microsoft is one among them which provides different services in maintaining the organizational data. The services can be accessed upon payment which is less in point of purchasing such huge data servers. However, the cloud environment is an loosely coupled one which does not pay more focus towards the user details. The user have the access can access the service. This encourages the malicious users in accessing the data to which they have no access.

The data security is more essential as the organization maintains various information like their business, customer and other details. The customer information should be stored and maintained in more secure manner as the organization is responsible for their privacy.

Revised Manuscript Received on October 05, 2019.

Kumaresan S, Research Scholar Dept. of Computer Science, Bharathiar University, Coimbatore, Tamil Nadu, India. s_kumaresan67cs@yahoo.com

Dr. Vijayaragavan Shanmugam, Professor and Head Dept. of Computer Science, Muthayammal Engineering College, Rasipuram, Tamilnadu, India. vijayaragaCSE@yahoo.com

Such data security has been enforced with different techniques like password based restriction, which uses only the password to access the service. Also, the access to the data has been enforced at service level which restricts the user according to the security key provided. Similarly, the data security can be enforced according to data level or attribute level. The attribute level scheme restricts the malicious access in different attribute level. To perform this, the method uses different keys for different attributes and so on. However, the methods suffer to achieve higher performance in data security.

In most situations, the user's access details have been maintained in form of profile. The user profile represents various information like their personal, and access details. By maintaining the user profile, the data attribute to which the user have access can be identified easily. The profile based approaches are very general and used in different articles. This paper presents a deviated one from the profile based approach which uses the taxonomy of attributes and the class based encryption. Instead of using attribute based encryption (ABE), which introduces higher network overhead in distributing the keys to the registered users; the class based encryption algorithm would reduce the overhead as it propagates only selected keys to the users. The number of keys being distributed has been reduced in this case which reduces the overall network overhead and improves the security performance as well as throughput.

The attribute taxonomy which is a medium which represent the most information related to the data points. The attribute taxonomy covers various information like the type of attribute, the range values of attribute, importance of attribute in different classes, and so on. According to the taxonomy, the importance of attribute can be measured. This would be useful in classifying the data attributes into several classes. By classifying the data attribute under different classes, the number of keys being used for data security can be minimized. This approach uses such a method and uses only limited keys according to the number of classes and the same is used to secure the data. The detailed algorithm is presented in the next section.

II. RELATED WORKS

Various data security methods are discussed earlier and this section briefs some of them related to the issue in this section.

In [1], the author presents a security framework for the IaaS towards virtual domain. The method enforces data security according to various domain and classifies the services related to different domain. The method enforces the data security from different platforms of remote.

In [2], the author presents a cloud computing platform (TCCP) which is trusted. The method enables different services in infrastructure with the help of amazon service provider.
In [3], the author presents a verifier which uses integrity proofs for the customers and enforces control abilities to protect their data and application in cloud environment.
In [4], a domain based protection scheme has been presented for the support of infrastructure services. The method also provides a reliable data sharing scheme with the use of XML based framework.
In [5], the author presents a data prefetching scheme for cloud environment. The storage servers performs the data prefetching instead of clients and based on the events the data has been sent to the clients.
In [6], the author evaluates the impact of energy consumption on different file systems. The method uses the File Bench generator to simulate the workloads. In [7], a bench marking file system has been used to review the different range of tools.11
In [8], the author presents a activity and standby modes of security which store the data in storage servers and intermediate one. If there is any lost in the server the data will be backed up from the intermediate servers.
To achieve security on infrastructure services an TPM orient scheme is presented in [9]. The method uses symmetric key to authorize the users and enforced by remote servers.
In [10], a symmetric encryption method is presented which is searchable. The method dynamically selects the keys and keywords for the encryption schemes. The method reduces the time complexity in encryption and decryption.
In [11], the author proposes storage and retrieval scheme for the privacy preservation with guarantees. The method enables the data to be stored in a distributed manner and allows searching them.
In [12], an reversible regional privacy protection algorithm has been proposed which has been used to compress the video. In [14], an attribute based access control algorithm is presented which uses different policies to encrypt the data and is highly flexible to maintain fine grained access control.
In [15], the author presents a detailed review on different security issues and the methods available to tackle them in detail.
In [16], an attribute access control to maintain deduplication by encrypting sensitive data in client side. The method produces higher data security.
In [17], a quantum based approach has been presented for the privacy preservation. The method encrypts the data items by using different keys. The method uses oracle Grower and offset encryption strategies to ensure the correctness of the data.
In [18], a two factor scheme for authentication is presented which provides feasibility to perform mutual authentication between different devices and the cloud.
In [19], the author presents a detailed review on various methods of security which handles various threats and approaches are compared in detail.

III. PROBLEM FORMULATION

The problem of data security has been discussed as follows: If there exist a data point D which has N number of dimension or attributes. Among N numbers, a user U would have N-p number of attribute access. Restricting the user U from accessing N-(N-p) attributes is the challenge here. The key set in previous approach is large and this should be reduced. By classifying the attributes under small set of classes, a small set of key set can be used. This reduces the overhead in key distribution.

1. CLASS BASED ENCRYPTION AND DECRYPTION WITH USER PROFILE TECHNIQUE

The class based approach maintains the taxonomy of attributes which covers the type of attribute, importance of data attribute, and so on. The method reads the attribute set and estimates the class sensitive measure (CSM) for each attribute towards the available classes. Based on the classified attributes, the method selects a methods under randomization technique. Similarly, the key towards the encryption decryption has been selected under the same randomization technique. The selected key has been used to perform communication with secure encryption and decryption. The detailed approach is discussed below:

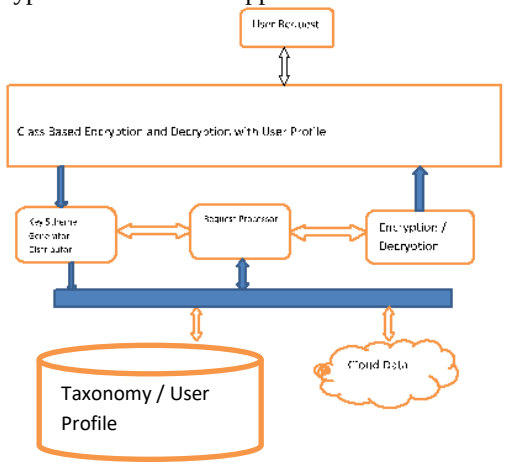

Figure 1: Architecture of CBE-UP Encryption algorithm

The functional architecture of proposed CBE-UP has been presented in Figure 1. It also shows the modules involved in the system.

2. Key/Scheme Generator and Distributor:

The key should be used and the scheme should be used for the secure data communication in cloud environment is performed in this stage. The attribute taxonomy and user profile has been read and searches the attributes and their type, importance and its profile factor. Using these values, the method estimates the class sensitive measure (CSM). Based on the CSM value, the method groups the attributes under N number of classes. For each class, the method select a key from key set and scheme from the scheme set. Selected key and scheme has been used to perform encryption and decryption in future.

Algorithm:
Input: Attribute Taxonomy AT, User Profile Up, Scheme Set Scs, Key set Ks
Output: Class Set Cs.
Start
Read AT, Up, Scs, Ks
For each attribute A from At
For each class C
Identify the type Atype = $\int_{i=1}^{size\ (AT)} AT(i).Type$

Identify Importance Aimp = $\int_{i=1}^{size\,(AT)} AT(i).Imp$

Identify profile factor Apf = $\int_{i=1}^{size\,(AT)} AT(i).pf$

Estimate CSM = $\frac{Atype \times 0.6}{C.Type \times 1.0} \times \frac{Aimp \times 0.8}{C.Imp \times 2.0} \times \frac{Apf \times 1.6}{C.pf \times 4.0}$

End

Choose the class with higher CSM.

Class C(A) = $\int_{i=1}^{size\,(C)} C(Max(CSM))$

Add attribute A to the Class C.

End

For each class C

Select a scheme Sch = $\int_{i=1}^{size\,(Scs)} Radom(Scs, i)$

Select a key k = $\int_{i=1}^{size\,(Ks)} Radom(Ks, i)$

End

Stop

The algorithm presented above explains how the attributes are classified under different classes to support higher data security. The method identifies the features of attribute from attribute set and for each of them, the method estimates the CSM value towards various classes. The method selects a class with maximum CSM value to index the attribute.

3. Request Processor:

The request received has been used to identify the list of attribute to be accessed to complete the request. Using the user profile, the method estimates the access strength measure (ASM) for each class attribute. The method decides the access grant or denying the request according to the value of ASM. If the user has higher value of ASM then the method identifies each class attribute to which he has access, and encrypts them using subsequent key allocated. Encrypted data has been given to the user.

Request Processor Algorithm:

Input: User Request Ur, Attribute Taxonomy AT, User Profile Up, Class Set C

Output: Result R

Start

Read user request Ur.

Identify list of attributes required Ar = $\int_{i=1}^{Size\,(AT)} \sum AT(i) \rightarrow Ur$

For each class C

Compute access strength measure ASM.

ASM = $\frac{\int_{i=1}^{size\,(Ar)} \sum Ar(i) \in Up(User)}{size\,(Ar)} \times \frac{\int_{i=1}^{size\,(C)} \sum C(i).Ar > Th}{size\,(c)}$

End

Compute cumulative ASM as CASM = $\frac{\sum_{i=1}^{size\,(C)} C(ASM)}{size\,(C)}$

If CASM>Th then

Original Data Od = Fetch the data from cloud.

Result R = Perform Encryption/Decryption.

Send result R.

End

Stop

The user request has been received and list of attributes are identified which must be accessed from the taxonomy. According to the attributes and the class, the method estimates the access strength measure (ASM) for each class to measure the cumulative value. Based on the value of CASM, the method decides to proceed with encryption or decryption to execute the service.

4. Encryption:

The data encryption is performed at the access request. The user request has been processed and evaluated for the user's access permission. Once the user clears the trust verification, the encryption process is performed. The original data fetched from the cloud by the service has been given here. The encryption algorithm has been invoked with the key set, original data, and the scheme set. For each attribute, the method identifies the key to be used, and scheme to be used. Using both of them, the method performs encryption accordingly. Similarly, for each class, the method uses different padding scheme as 0's and 1's. The number of 1's and 0's is decided according to the scheme.

Algorithm:

Input: Data Point Dp, Key Set Ks, Scheme Set Scs, Attribute Access Aa

Output: Result R.

Start

Read data point Dp.

Initialize duplicate Ad = $\int_{i=1}^{size\,(Dp)} \sum Dp(i) \in Aa$

For each attribute A

Identify the key Ak = $\int_{i=1}^{size\,(Ad)} Ks(Ad(i))$

Identify the scheme As = $\int_{i=1}^{size\,(Ad)} Scs(Ad(i))$

Result R=Perform Encryption.

If As is Polynomial then

Perform Padding with number of 0s of size Ak

Else

Perform padding with number of 1's of size Ak

end

End

Stop

The above discussed algorithm show how the encryption is performed. The list of attributes are identified which are allowed to access by the user. For the identified attributes, the method identifies the scheme and key using which the encryption is performed. Encrypted result has been produced as result to the user.

5. Decryption:

The user receives the encrypted data from the cloud service. According to the attributes to which the user has access, the method identifies the list of schemes and keys. Using the key and scheme identified for each attribute, and performs decryption to achieve the original data. Initially, the method removes the padding attached according to the scheme and key used.

Algorithm:

Input: Key set Ks, Attribute Set As, Encrypted Data Ed, Scheme Set Scs

Output: Original Data OD.

Start

Read Encrypted Data Ed.
Byte Data Bd = Split Data into Number of Bytes

For each attribute A
Identify scheme S.
If S is Polynomial then
Remove padding of number of 0s of size key
Original Data OD(A) = Perform Decryption
Else
Remove padding of number of 1s of size key
Original Data OD(A) = Perform Decryption
End
End
Stop

The above discussed algorithm shows how the data decryption is performed. The decryptor algorithm receives the user service request and identifies the service and the data submitted. Then the list of attributes of the service is identified and their consequent padding details and key are identified. Using them, the original text is obtained by decrypting the text.

IV. RESULT AND DISCUSSION

The proposed class based attribute encryption standard with user profile method is implemented and evaluated for its efficiency in different parameters. To evaluate the performance of the proposed algorithm, various parameters has been considered. The method has produced efficient result in Tampering and security performance.

Parameter	Value
No of Users	100
No of services	50
No of Attributes	200
Protocol	CPE-UP
Tool Used	Advanced Java

Table 1: Simulation Details

The details of simulation used for the performance evaluation is presented in Table 1. The result produced by the TAM algorithm is presented below.

Techniques	Tampering Efficiency %		
	50 Services	75 Services	100 Services
ABFD	72	67	65
TAMM	77	83	89
CBE-UP	79	86	93

Table 2: Comparison of Tampering efficiency on different no of services

The Performance analysis on tampering resistance has been presented in Table 2. The CPE-UP algorithm has improved the Tampering resistance than ABFD and TAM approach in all the conditions.

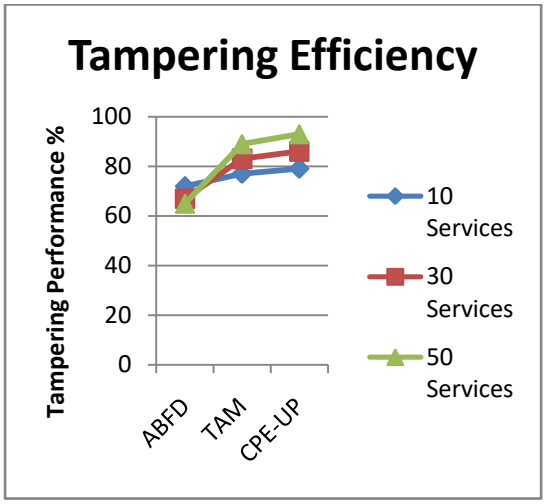

Figure 2: Comparison of Tampering efficiency

The performance on Tampering efficiency is measured and presented in Figure 2. The evaluation is carried out with different number of services. The proposed CPE-UP algorithm has produced higher efficiency than the ABFD and TAM algorithm in all the conditions.

Techniques	Security Efficiency %		
	50 Services	75 Services	100 Services
ABFD	65	69	78
TAM	77	83	89
CPE-UP	81	86	92

Table 3: Comparison of security efficiency on different no of services

The performance on security has been measured and presented in Table 3. The evaluation is carried out with different number of services. The proposed CPE-UP algorithm has improved the security efficiency than ABFD and TAM approach in all the conditions.

Figure 3: Comparison on security performance

The Figure 3, shows the efficiency of security produced by the two methods in varying number of services. The result shows that the proposed CPE-UP algorithm has produced higher efficiency than the ABFD and TAM algorithm.

Techniques	Network overhead in bytes		
	50 Services	75 Services	100 Services
ABFD	72	86	89
TAM	65	67	71
CPE-UP	52	56	62

Table 4: Comparison of network overhead on different no of services

The Table 4, shows the comparison result on network overhead in different number of services. The proposed CPE-UP algorithm has reduces the network overhead than ABFD and TAM approach in all the conditions.

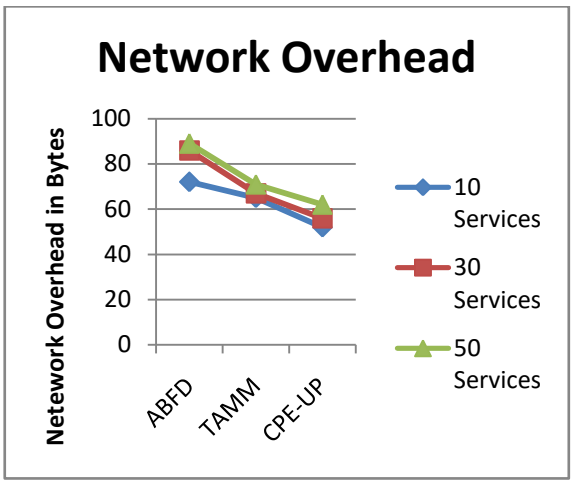

Figure 4: Performance on network overhead

The performance on network overhead is measured and presented in Figure 4. The proposed CPE-UP algorithm has produced less overhead than the previous ABFD and TAM algorithm.

Techniques	Time complexity in seconds		
	50 Services	75 Services	100 Services
ABFD	46	67	86
TAM	21	32	39
CPE-UP	17	24	32

Table 5: Comparison of time complexity on different no of services

The Table 5, shows the comparison result on time complexity in different number of services. The proposed CPE-UP algorithm has reduces the time complexity than ABFD and TAM approach in all the conditions.

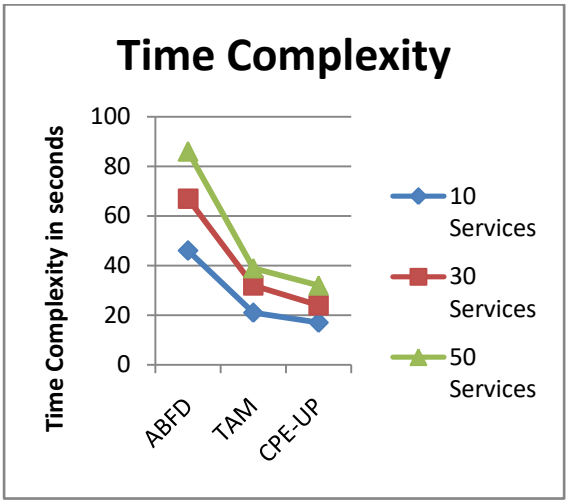

Figure 5: Performance on time complexity

The performance on time complexity has been measured and compared with the results of other methods. However, the proposed CPE-UP algorithm has reduced the time complexity in all the number of services than the previous ABFD and TAM algorithm.

V. CONCLUSION

The performance of cloud data security has been analyzed and discussed in detail in this paper. To improve the security performance an efficient class based encryption with user profile is presented. The method first groups the attributes of the class according to the importance and type of attribute from the attribute taxonomy. The method estimates the class sensitive measure to group the attributes under different classes. Then the method receives the user request and identifies the list of attributes and their key and their access rights to the user. According to them, the method estimates the access strength measure (ASM) towards each class to compute the cumulative value. Based on the value of CASM, the method accepts or denies the access. The data retrieved from the cloud has been encrypted with different keys according to the scheme and attribute. Encrypted key has been padded with different method to produce the result. The user can decrypt the data and remove the padding to produce the original data. The method generates efficient result on all the parameters considered than the previous algorithms.

REFERENCES:

1. Nicolae Paladi, Providing User Security Guarantees in Public Infrastructure Clouds, IEEE Transaction on cloud computing, vol. 5, issue 3, 2017.
2. N. Santos, "Towards trusted cloud computing", Proc. Conf. Hot Topics Cloud Comput., pp. 3, 2009.
3. J. Schiffman, T. Moyer, "Seeding clouds with trust anchors", Proc. ACM Workshop Cloud Comput. Security, pp. 43-46, 2010.
4. N. Paladi, A. Michalas, "Domain based storage protection with secure access control for the cloud", Proc. Int. Workshop Security Cloud Comput., pp. 35-42, 2014.
5. 5. Jianwei Liao ; Performing Initiative Data Prefetching in Distributed File Systems for Cloud Computing, IEEE Transaction on cloud computing, vol. 5, issue 3, 2017.
6. P. Sehgal, "Evaluating performance and energy in file system server workloads", Proc. 8th USENIX Conf. File Storage Technol., pp. 253-266, 2010.

7. V. Tarasov, "Benchmarking file system benchmarking: It* is* rocket science", Proc. 13th Workshop Hot Topics Operating Syst., pp. 1-5, 2011.
8. J. Liao, "Partial replication of metadata to achieve high metadata availability in parallel file systems", Proc. 41st Int. Conf. Parallel Process., pp. 168-177, 2012.
9. B. Bertholon, "Certicloud: A novel TPM-based approach to ensure cloud IaaS security", Proc. IEEE Int. Conf. Cloud Comput., pp. 121-130, 2011.
10. S. Kamara, "Parallel and dynamic searchable symmetric encryption" in Financial Cryptography and Data Security, New York, NY, Springer, pp. 258-274, 2013.
11. Jingwei Li ; Towards Privacy-Preserving Storage and Retrieval in Multiple Clouds, IEEE Transaction on cloud computing, vol. 5 issue 3, 2017.
12. Xiaojing Ma ; Fully Reversible Privacy Region Protection for Cloud Video Surveillance, IEEE Transaction on Cloud computing, vol.5 issue 3, 2017.
13. Rohit Ahuja ; A Scalable Attribute-Based Access Control Scheme with Flexible Delegation cum Sharing of Access Privileges for Cloud Storage, IEEE Transaction on cloud computing, vol. issue 99, 2017.
14. Rajesh Yadav, A Critical Review of Data Security in Cloud Computing Infrastructure, International Journal of Advanced Studies of Scientific Research, Volume 3, Issue 9, 2018.
15. Taek-Young Youn, Authorized Client-Side Deduplication Using CP-ABE in Cloud Storage, Hindawi, Wireless Communications and Mobile Computing, Volume 2019.
16. Wenjie Liu, A Quantum-Based Database Query Scheme for Privacy Preservation in Cloud Environment, Hindawi, Security and Communication Networks, Volume 2019.
17. Jiaqing Mo, An Efficient and Provably Secure Anonymous User Authentication and Key Agreement for Mobile Cloud Computing, Hindawi, Wireless Communications and Mobile Computing, Volume 2019.
18. Dhivya R, Security Attacks Detection in Cloud using Machine Learning Algorithms, IJRET, 6,2,2019.
19. Mohammad Aazam ; Eui Nam Huh Inter-cloud Media Storage and Media Cloud Architecture for Inter-cloud Communication, 2014 IEEE 7th International Conference on Cloud Computing

AUTHORS PROFILE

Mr. Kumaresan. S Research Scholar Dept of Computer Science, Bharathiar University, India had graduated from University of Madras, India and Completed Master Degree from Bharathidasan University, India. My research includes Cloud Computing and Cloud Technologies. Another Master degree from Periyar University, India. I am life member in ISTE.

Dr. Vijayaragavan Shanmugam, had received graduation from University of Madras and completed post-graduation and Ph.D., from Anna University, India. He is presently with Muthayammal Engineering College, Tamilnadu, India as a Professor& Head. His research interests include Mobile Computing, Cloud Computing, Data Mining and Mobile Application Development. He is a life member in ISTE and CSI