ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Review on Cost Effective and Dynamic Security Provision Strategy of Staging Data items in Cloud

Praveen Kumar Rajendran, K Manoj Kumar, Tejasree S, and R Aswini

[1]Cognizant Technology Solutions, Chennai. India
[2,3]Assistant Professor, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering Tirupati, India
[4]Assistant Professor, Department of Computer Science, IFET College of Engineering, Villupuram, India

ABSTRACT

Cloud computing is a thriving technology that relies on sharing computing resources rather than having a local server in order to handle the application. Cloud usually uses the phrase of "pay as you go" to describe its functionality. The security issue is the major concern in data interchange since the entire user cannot pertain to access all the data from the server. In this paper, Cost Effective and dynamic Security Provision strategy of Staging Data items in the cloud has been proposed. The concept of utilizing staging data items rather than direct cloud access is taken as the core idea to reduce the cost of utilization as well as the concept of Anonymization is discussed that reduces the size of data utilization and behaves as the security provision strategy according to the severity of the data to per users. The effective check taken in the projected approach is a flow time monitoring to provide the cost reduction and security enhancing scheme in a dynamic way.

Keywords*:* Anonymization, Intermediate data, Severity, Cloud, Security

Corresponding author

ISSN: 0975-8585

INTRODUCTION

In the recent trend of technological world, Cloud is acting as the predominant technological area that serves globally. It is the boon to the entire sector worldwide as they can utilize the platform, software's and application by renting the server as a subscriber or reseller from the service providers only by the means of internet [15]. Through the provision of cloud service such as Limitless flexibility, Better Reliability provisions, enhance collaboration, Portability, Simpler devices satisfies its consumer globally with the advent growth of technical support to its consumers, a constraint can pertain to think from the common man's perspective as the reason of the renting cost of utilizing time and size of the data by the cloud provider [14]. Its service provisions are vibrating as the Cloud computing areas are taken as commercial computing that provide better accessibility to high-performance computing [20]. The major advantage of Cloud Computing is the resources can be accessed anywhere, anytime by an organization [18]. A widespread view is that utilizing cloud computing will save money. Many statistical reports argue in the same wavelength though provisions of cloud are highly satisfactory. That analysis put forward that the utilizing of cloud will save money is uncertain for research computing. On a pure price comparison, the more powerful cloud computing instances, rented on an hourly basis, appears to be one-and-a-half to two times more expensive per core-hour. [1]. The main characteristic of the cloud service is "Pay as you go manner" [10][16]. An analysis depicts that only the provision of cost, convenient cloud is not only permissible to the consumer expectation, but it also has a strict strategy to preserve the user's data. This is the most focused discussion on cloud securable service provision of today as it lies on the fact that customer trust towards the service provider is a must with a value to data confidentiality, integrity and faultlessness. [2][3] Since security is an important concern, accessibility to high severity data of a consumer by third party sector for analysis may also come under the data insecurity. From the analysis made by Praveen et al [19] [18] proposals it is found that intrusion is one of the serious issues which has to be addressed in any type of network.

This paper refers to two distinct strategies of cloud data utilization. The strategy is to provide a cost effective utilization of data by analyzing the frequency data tables and providing accessibility through the staging data items as that avoids the direct access to the cloud, hence cost effective. The second strategy is to preserve the data by identifying the severity of the data and providing accessibility to privileged consumers and end users according to their ownership. The second strategy uses the concept of severity segregation and Anonymization to preserve and reduce the data size; hence it provides data security and reduces the cost of utilization. The projected approach of this paper is to dynamically evaluate the frequent data's in the staging data items to preserve against impersonal accessibility and to reduce the cost of utilization.

RELATED WORKS

Cloud computing obviates the necessity for application developers to apprehend themselves in the midst of the logistics and cost matters of hefty blunt infrastructure stash instead of another service application developer. [6] The current lively auditing utilization of the multiple cloud is quite inefficient, and since it is consequently preserving the data in the cloud. The major challenge for research scholars is to provide a security for the transactions made in cloud [11]. This research paper focus on important technique of Secure Dynamic Auditing Protocol sharing among users of service providers, to share the accredited cloud over batch auditing service providers. [4] Within this cloud, unified framework proxy servers are deployed on cloud hosting sites. Conversely, proficient content allotment paths must be also deployed, while the underlying results to typically consume resource heterogeneity.[5] View and trend current for the future costs based on the optimized functional knowledge of scaling applications are also literally incorporated in this constraint.[6] wherein the Computation-storage trade off in highly practical approach toward achieving minimum data Sets just as an Internet service provider will count on a single network provider, over computational cost effectiveness and also it perhaps a cloud user should not depend on a single cloud service provider either.[7]

STRUCTURAL REPRESENTATION

Fig 1 depicts the structural representation of the projected approach. A clear view of the concept integrated to prove the strategy taken under consideration is designed initially.

ISSN: 0975-8585

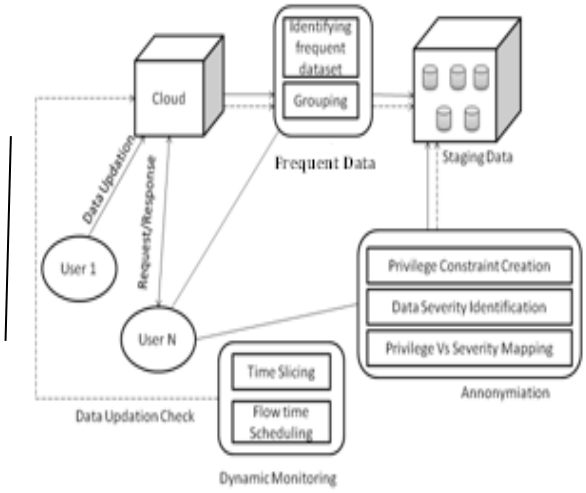

Fig 1: Structural Representation of Projected Approach

It comprises of set of Modules to complete the study postulated. At first the Analysis of frequently utilized data in the cloud to annoymize the data from the staging data items with the principle of Privilege constraint creation, Data Severity Identification and Privilege Vs Severity Mapping. A dynamic Monitored is used to set a time slicer for monitoring the data updating to follow up the sets of data staging and privacy preserving.

A. Analysis of frequently Utilized Data

The data in the cloud are investigated for its frequent accessibility, so as to move the datasets to the staging data items that acts as the staging server for the cloud. The purpose of the staging server maintains the frequently accessed data of the cloud; this can be owned by a private or public sector as a reseller to provision the subscriber in all real-time scenarios. The process step of this stage includes analysis of frequently utilized data item set by finding out the dataset frequently accessed in a cloud database. In order to identify the frequent dataset accessed, a minimum support is applied that satisfied the consumer need are filtered out and stored as the resultant of minimum support bound of the customer. The resultant of the minimum bound is attained count is then applied to the procedure of minimum confidence constraint that frames certain rules to filter out the data in a well organized manner. According to the principle of association rule, identifying all frequent item set in a database is quite complicated in view of the fact that it involves searching all possible item set. The search represented in this method uses the principle of item grouping. The Possible data items are the Power set over the data item, removing the nullable dataset. The set of possible data item is I that have the size 2n-1. The search of exponentially increase in data items are done with the downward closure property. This step of the system reduces the cost of accessing the data, since the system does not access the cloud directly and it accesses the staging data items.

B. Constraint Creation

A privilege of delegation authorization over the staging data items is framed according to the type of data organized in the dataset. For a better example, we took an experimental analysis of the hospital dataset for our projected work. Wherein the doctors are considered to be highly privileged users, Guardian or other friends of the patients are low privileged users, the application user is the medium privileged users. A constrain based view creation; depending upon the type of privileged user is framed according to the severity of the dataset present in the staging data items.

ISSN: 0975-8585

Table 1.1 Overall hospital management sample table.

Id	Patient Name	Monthly Salary	Disease
S5001	Duke	$250	Dengue
S5002	Morris	$300	HIV
S5003	Sam	$180	Hepatitis
S5004	Mike	$200	Cancer
S5005	David	$500	Ebola

The high severity column is Type of Disease, the low severity column is the name of the patient and the medium severity column is the salary of the patient.

The entire data set of the table is analyzed to segregate the severity of the column according to the privilege categorization. The segregation of the dataset is done by the process of filtering the mandatory column and non-mandatory column according to the category of privilege the user owns.

C. Anonymization

According to the definition from Wikipedia, "Data anonymization is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous" [12]. In the projected approach, data Anonymization is made to the categorization of the privileged user with respect to the severity of the dataset as depicted in the Table 1.2

Table 1. 2: Data anonymization

User\severity	High	Medium	Low
High	visible	visible	visible
Medium		visible	visible
Low			visible

This step preserves the data from leakage during the referential integrity of the tables in the intermediate database as well as during the normal accessibility of the data from the staging data items. Apart from preserving the data, this step also reduces the size of the data being accessed by the set of privileged user, thus reduces the cost of utilization since the size is reduced.

D. Dynamic Evaluation

Dynamic Evaluation is the core idea of the proposed approach on the illustrated and implemented ideas of the various cloud computing scenarios. The base concept provide this approach cost effective and security provision scheme in a different approach, but they fail to monitor the cost reduced and privacy preserving schemes in a dynamic manner. The main proposal of this paper is a Dynamic flow monitoring strategy that monitors the server for its frequently accessed data for every n seconds. Where the n value is taken as 2880.This n value acts as the rotational time slice of server monitoring. The analyzed frequent datasets are imposed with the further steps of Anonymization.

ALGORITHM

A.Algorithm

The proposed concept is implemented using the following algorithm, which is followed by the detailed description about the implementation of the algorithm

Algorithm 1: Cost Effective and Dynamic Provision Strategy Algorithm

ISSN: 0975-8585

Input:

1. Data Item I
2. Grouping Category Gn

```
1.  Input the Data Item D
2.  {
3.  Initiate Analyze Frequent Data Item
4.  {
4.1 For Each a belongs to Data Item D[]
 4.2  Insert I[] into Grouping Category GN
 4.3  For Each b belongs to Data Item D[]
 4.4  Insert D[] into Grouping category GN
 4.5  }
5.  {
6.  Initiate Constraint Creation
 6.1  Set User Privileges,
      P(U) ← GN belongs to (Ga,Gb,…Gn)
      Where P(U)=User Privileges
      }
7.  {
8.  Initiate Annoymization
 8.1  GN=(Ga,Gb,…Gn) set (Aa,Ab…An) belongs to AN
      Annoymization
 8.2  }
9.  {
10. Initiate Dynamic check
 10.1 Set Dynamic check (Dc)= 2880sec
 10.2 For each (Dc)
 10.3 Loop through step 2 to step 4
 10.4 }
 11. End;
12. }
```

Output:

1. Increase in A_N Tends to decrease in S(I[ ])
2. Decrease in S(I[ ]) Decreases Cost(D_u)

The Algorithm formulates the entire flow of the projected work. It inputs the Data item from the server and Group category represented as G_N. The Process Flow in such a way analyzing the frequent data item that belongs to the Input data item. The resulted input data are stored in the data staging server. The concept of grouping and constraint creation for the users and the data has been carried out for securing the data in the staging server. Users are clustered according to the designation and pertain to certain group (Ga, Gb,…Gn) according to the privileges of the User P(U).A set of severity has been framed as stated in the concept of above table 1.1 and annoymization is made according to the table 1.2 for the user according to P(U) with the concept of Data hashing.

A dynamic monitor has been introduced in this paper that differentiates our work from the base idea for securing and reducing the cost for each updating occurrence in the server. implementing the projected approach will prove that, reducing the utilization size by anonymization will reduce the cost and maintain the privacy of the data according to the severity.

DISCUSSION

This paper takes, Xuyun Zhang et al [9] has base work which incorporates the concept of this paper and worked on its idea by adding a Dynamic Monitoring strategy as that paper approach was static monitoring with its concept of Cost reduction and security provision. The details about the data updating on

the server and the flow of annoynimization and security loopholes after the data updating has not been taken into consideration in the base paper. Thus our system proposes a solution to the constraint that rose in the base paper by introducing the concept of dynamic monitoring for keeping track the data updating as well as to reduce the cost and to provide security provision in the staging data server in timely manner.

CONCLUSION

Thus the Cost Effective and dynamic Security Provision strategy of Staging Data items in cloud has been proposed with the effective concept to optimize the existing scenarios. It also seems to be a cost effective and securable data utilization strategy with its concept oriented and algorithmic approaches as the result of the proposed scenarios is much better than the existing scenarios. Analysis is a proven solution to reduce the cost and security constraints. Future studies will investigate archiving concepts of the examined staging data items and implement the proposed idea.

REFERENCES

[1] Marco Balduzz, Jonas Zaddach, A Security Analysis of Amazon's Elastic Compute Cloud Service– Long Version; 2011

[2] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, Journal of Internet Services and Applications 2013; 1-13.

[3] Frederick R. Carlson, arXiv preprint arXiv: 1404.6849 (2014).

[4] Yang, Kan, and Xiaohua Jia. Parallel and Distributed Systems, IEEE Transactions 2013; 24(9): 1717-1726.

[5] Kimish Patel , Nvidia Corporation, Santa Clara Murali Annavaram , Massoud Pedram, Computers, IEEE Transactions 2013; 62(9): 1772-1785.

[6] Yuan Tian, Chuang Lin, Zhen Chen_, Jianxiong Wan, and Xuehai Peng Tsinghua Science and Technology 2013; 18(3): 298-307.

[7] Chaisiri, Sivadon, Bu-Sung Lee, and Dusit Niyato. Services Computing, IEEE Transactions 2012; 5(2): 164-177.

[8] Yuan, Dong, et al. IEEE Transactions on Parallel and Distributed Systems 2013; 24(6): 1234-1244.

[9] Zhang, Xuyun, et al. Parallel and Distributed Systems, IEEE Transactions 2013; 24(6): 1192-1202.

[10] B. R. Kandukuri, R. V. Paturi and A. Rakshit, IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009.

[11] Data Anonymization, http://en.wikipedia.org/wiki/Data_anonymization.

[12] Lydia Jeba, M.Rathna, International Journal of Applied Engineering Research", December 2014

[13] Sudha Devi and Thilagavathy, Asian Journal of Information Technology 2013, 12(9):305-311.

[14] Nathaneal Ramesh, J. Andrews, Indian Journal of Science and Technology, 2015;8(4), 301-306.

[15] B. R. Kandukuri, R. V. Paturi and A. Rakshit, IEEE International Conference on Services Computing, Bangalore, India,2009; September 21-25.

[16] P.Neelaveni and M.Vijayalakshmi, Asian Journal of Information Technology, 2014; 13(6):320-330.

[17] Praveen Kumar Rajendran, B.Muthkumar, G.Nagarajan, Procedia Computer Science 2015; 48,325-329.

[18] Rajendran, Praveen Kumar, M.Rajesh, R.Abhilash. Indian Journal of Science and Technology 2015; 8(35).

[19] Rajendran, Praveen Kumar, B.Muthukumar, S.Murugan, G.Nagarajan, Advances in Intelligent Systems and Computing, Springer International Publishing.

[20] Rajesh, M., R. Abhilash, and R. Praveen Kumar. International Journal of Electrical and Computer Engineering (IJECE) 2016; 6(3).

[21] Rajendran, Praveen Kumar. Indian Journal of Science and Technology 2016; 9(31): 1-6.

[22] S.L. Jany Shabu and Manoj Kumar.K. International Journal of Applied Engineering Research (IJAER) 2014; 9(22): 16269-16276.

[23] Manoj Kumar.K. WSEAS Transactions on Advances in Engineering Education 2016; 13: 1-6.